Wigner Functions and Separability for Finite Systems

Arthur O. Pittenger and Morton H. Rubin

Department of Mathematics and Statistics and Department of Physics

University of Maryland, Baltimore County, Baltimore, MD 21250[*]

(Dated: February 1, 2008)

Abstract

A discussion of discrete Wigner functions in phase space related to mutually unbiased bases is presented. This approach requires mathematical assumptions which limits it to systems with density matrices defined on complex Hilbert spaces of dimension p^n where p is a prime number. With this limitation it is possible to define a phase space and Wigner functions in close analogy to the continuous case. That is, we use a phase space that is a direct sum of n two-dimensional vector spaces each containing p^2 points. This is in contrast to the more usual choice of a two-dimensional phase space containing p^{2n} points. A useful aspect of this approach is that we can relate complete separability of density matrices and their Wigner functions in a natural way. We discuss this in detail for bipartite systems and present the generalization to arbitrary numbers of subsystems when p is odd. Special attention is required for two qubits ($p = 2$) and our technique fails to establish the separability property for more than two qubits. Finally we give a brief discussion of Hamiltonian dynamics in the language developed in the paper.

PACS numbers: 03.65.-a, 03.65.Ca, 03.65.Fd

[*]Electronic address: rubin@umbc.edu, pittenge@math.umbc.edu

I. INTRODUCTION

In a study of thermal equilibrium of quantum systems [26], Wigner introduced the famous function that now bears his name. There is an extensive literature on the Wigner function for continuous variables [6, 9]. The literature on discrete Wigner functions is less extensive, but the importance of discrete phase space in quantum information has revived interest in the subject [8, 17, 24]. In particular, the paper by Gibbons, *et. al.* contains a useful list of references.

In this paper we present a discussion of discrete Wigner functions in phase spaces related to mutually unbiased bases (MUB). Our approach differs from the geometric method of Wootters in being more operational and closer to the methodology of the continuous case [8, 28], but our approach also requires mathematical assumptions which limits it to systems with density matrices defined on complex Hilbert spaces of dimension p^n where p is a prime number. With this limitation it is possible to define phase space and Wigner functions which mimic the continuous case. There does not seem to be any simple way to do this for other dimensions, see for example [13, 23]. A useful aspect of this approach is that we can relate the separability of density matrices and their Wigner functions. We discuss this in detail for bipartite systems and present the generalization to arbitrary numbers of subsystems. As an application of our analysis, we show that for p an odd prime, with a particular choice of "phase" parameters, Hermitian operators used in [8] for n $p-$level systems are tensor products of opeators for the individual $p-$level subsystems.

The paper is organized as follows. We first briefly review the definition and properties of the Wigner function for continuous variables and list the most important properties that are retained in the discrete case. Our discussion of the discrete Wigner function makes extensive use of generalized spin matrices which are defined in the section III for a singl particle. In order to determine a suitable choice of phase space, we are led to consider mutually unbiased bases, and this is done in sections IV and VI, and further discussed in Appendix X B. The discrete Wigner function for a single particle is then defined and its properties discussed in section V. The generalization of our discussion to more than one particle begins with section VI. The transition to the general case is aided by using the geometry of discrete phase space, which is summarized in Appendix X E. In section VII D we generalize the Wigner function to dimension p^2, and in VIII to p^n.

The problem of separability when $p = 2$ requires special treatment, and in section VII the case of two qubits is analyzed. The generalization to more than two qubits appears to be impossible by the present technique, this is discussed in section VIII. Finally, in section IX a brief discussion of Hamiltonian dymanics is presented and a simple example using MUB is given. Various background and technical issues are discussed in the appendices, including the positivity of the density matrix.

II. WIGNER FUNCTION FOR A PARTICLE MOVING IN ONE DIMENSION

Let ρ be the density matrix for a particle moving in one dimension, and let Q and P be the position and momentum operators for the particle. We set $\hbar = 1$ so the Heisenberg commutation relation is $[Q, P] = i\mathbf{1}$. It is convenient to introduce the Wigner function as the Fourier transform of its characteristic function χ, defined by

$$\chi_\rho(u, v) = tr\left[\rho D(u, v)\right] \tag{1}$$

where D is the unitary translation operator

$$D(u, v) = e^{-i(uP - vQ)} = e^{-iuP}e^{ivQ}e^{iuv/2}. \tag{2}$$

These operators form a projective group called the Heisenberg-Weyl group [25]. It is easy to show that

$$D(u, v)D(a, b)D(u, v)^\dagger = e^{i(a,b)\circ(u,v)}D(a, b), \tag{3}$$

where the phase factor is the symplectic product of the operator "indices",

$$(a, b) \circ (u, v) = bu - av. \tag{4}$$

The Wigner function is defined by

$$\begin{aligned} W_\rho(q, p) &= \frac{1}{(2\pi)^2}\int_{-\infty}^{\infty} du \int_{-\infty}^{\infty} dv \chi_\rho(u, v)e^{-i(qv-pu)} \\ &= \frac{1}{(2\pi)^2}\int_{-\infty}^{\infty} du \int_{-\infty}^{\infty} dv tr\left[\rho D(u, v)\right]e^{-i(qv-pu)}. \end{aligned} \tag{5}$$

To see that this agrees with the standard definition let us compute the trace in the last equation using a complete set of eigenvectors of Q,

$$W_\rho(q, p) = \frac{1}{(2\pi)^2}\int du \int dv \int dx \langle x|\rho|x + u\rangle e^{ivx}e^{iuv/2}e^{-i(qv-pu)}$$

where Eq. (2) was used with

$$e^{-iuP}|x\rangle = |x + u\rangle.$$

Doing the v and x integrals gives

$$
\begin{aligned}
W_\rho(q,p) &= \frac{1}{2\pi}\int du \int dx \langle x|\rho|x+u\rangle \delta(x + \frac{u}{2} - q)e^{ipu} \\
&= \frac{1}{2\pi}\int du \langle q - u/2|\rho|q + u/2\rangle e^{ipu}.
\end{aligned}
\tag{6}
$$

The definition of the operators $D(u,v)$ is not unique. There is some freedom in the choice of phase, referred to as gauge freedom in reference [25], p 181. While the choice used here is the standard one, the issue is not so simple for the discrete case.

Many of the standard properties of the Wigner function can be deduced readily from Eq. (5):

1. the mapping $\rho \to W_\rho$ is convex linear,

2. W_ρ is normalized, $i.e.$

$$\int dq \int dp W_\rho(q,p) = 1$$

which follows from $\chi_\rho(0,0) = tr\rho = 1$,

3. W is real since $\chi_\rho^*(u,v) = \chi_\rho(-u,-v)$,

4 . if $\rho' = D(a,b)^\dagger \rho D(a,b)$ then

$$
\begin{aligned}
W_{\rho'}(q,p) &= \frac{1}{(2\pi)^2}\int du \int dv tr\left[\rho D(a,b)D(u,v)D(a,b)^\dagger\right]e^{-i(qv-pu)} \\
&= \frac{1}{(2\pi)^2}\int du \int dv tr\left[\rho D(u,v)e^{i(ub-va)}\right]e^{-i(qv-pu)} \\
&= W_\rho(q+a,p+b),
\end{aligned}
$$

5. the marginal distributions are probability densities,

$$
\begin{aligned}
\int_{-\infty}^{\infty} dq W_\rho(q,p) &= \langle p|\rho|p\rangle \\
\int_{-\infty}^{\infty} dp W_\rho(q,p) &= \langle q|\rho|q\rangle.
\end{aligned}
$$

More generally, if we integrate along a line in phase space we get a probability density

$$\int_{-\infty}^{\infty} dq \int_{-\infty}^{\infty} dp W_\rho(q,p)\delta(q\cos\theta + p\sin\theta - q_0) = \langle q_0;\theta|\rho|q_0;\theta\rangle,$$

where $|q_0;\theta\rangle$ is the eigenvector of $Q_\theta = Q\cos\theta + P\sin\theta$ with eigenvalue q_0.

4

Finally, to show that the Wigner function is equivalent to the density matrix, we write the density matrix in terms of the Wigner function. This is done easily by taking the inverse Fourier transform of Eq. (6)

$$\langle q|\rho|q'\rangle = \int_{-\infty}^{\infty} W_\rho(\frac{q+q'}{2}, p)e^{-ip(q-q')}dp.$$

It follows from this equation that

$$tr\,[\rho_1\rho_2] = 2\pi \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} dpdq W_{\rho_1}(q, p)W_{\rho_2}(q, p),$$

which is just Plancheral's theorem.

Proving that a given function $W(q, p)$ corresponds to a density matrix comes down proving that the inverse formula leads to a ρ which is positive (cf. ref [16]).

Finally we note that we can define a Wigner function, W_A, for any operator A for which Eq. (5) is defined.

III.   GENERALIZED SPIN MATRICES

We briefly review some facts about the generalized spin matrices which are of interest here and introduce some notation that will be used throughout the paper. We shall use letters j, k, s, t to denote elements of $Z_d = \{0, 1, \cdots, d-1\}$, the integers modulo d. Let H_d be a d-dimensional complex Hilbert space, and let $\{|k\rangle, k \in Z_d\}$ be an orthonormal basis of H_d. Let M_d be the vector space of complex $d \times d$ matrices that act on H_d. This space is a d^2-dimensional Hilbert space with respect to the Frobenius or trace inner product

$$\langle A, B \rangle = tr\left(A^\dagger B\right) \tag{7}$$

for $A, B \in M_d$. The set of matrices $\{|j\rangle\langle k|, j, k \in Z_d\}$ is an orthonormal basis of M_d. Let $\eta = \eta_d = e^{i2\pi/d}$, and define the generalized spin matrices as the set of unitary matrices

$$S_{j,k} = \sum_{m=0}^{d-1} \eta^{jm}|m\rangle\langle m+k| \tag{8}$$

where index addition is to be understood to be modulo d. This set of d^2 matrices, including the identity matrix $I = S_{0,0}$, forms an orthogonal basis of M_d [19].

It is not difficult to show that

$$S_{j,k}^\dagger = \eta^{jk}S_{-j,-k} \tag{9}$$

$$S_{j,k}S_{s,t} = \eta^{ks}S_{j+s,k+t}. \tag{10}$$

5

From Eq. (10) it follows that $S_{j,k}$ and $S_{s,t}$ commute if and only if the symplectic product $(j,k) \circ (s,t) = 0$, where

$$(j,k) \circ (s,t) \equiv ks - jt \mod d \tag{11}$$

which should be compared with Eq. (4). We also will need the relation

$$S_{j,k}^m = \eta^{m(m-1)jk/2} S_{mj,mk}, \tag{12}$$

The spin matrices can be generated from two matrices: $S_{1,0}$ which is diagonal, and $S_{0,1}$ which is real and translates each state to the next lowest one modulo d. One can check that $S_{j,k} = S_{1,0}^j S_{0,1}^k$. These spin matrices can be viewed as translation operators in a manner similiar to the $D(u,v)$ operators for the single particle discussed in section II. The analog to property 4 is

$$S_{s,t} S_{j,k}^m S_{s,t}^\dagger = \eta^{m(tj-sk)} S_{j,k}^m = \eta^{m(s,t) \circ (j,k)} S_{j,k}^m. \tag{13}$$

Since the matrices $\{\frac{1}{\sqrt{d}} S_{j,k}\}$ form an orthonormal basis on the d^2-dimension Hilbert space M_d, they satisfy the completeness relation

$$\frac{1}{d} \sum_{j,k=0}^{d-1} S_{j,k} \, tr(S_{j,k}^\dagger A) = A, \tag{14}$$

where $A \in M_d$. This set of spin matrices has appeared repeatedly in the mathematics and physics literature, for example [4, 5, 11, 19, 21, 27] among others, and is often also referred to as the (discrete) Heisenberg-Weyl group.

Finally we define a set of orthogonal one-dimensional projection operators that we will need. Let p be a prime number. For $(j,k) \neq (0,0)$ and $0 \leq r \leq p-1$

$$P_{j,k}(r) = \frac{1}{p} \sum_{m=0}^{p-1} (\alpha_p(j,k) \eta^r S_{j,k})^m \tag{15}$$

where $\alpha_2(1,1) = -e^{i\pi/2}$ and $\alpha_p(j,k) = 1$ otherwise is a set of orthogonal one dimensional projection operators [19]. If we make this definition for d not prime, we find that we generate rank 1 projection operators which are not orthogonal. The reason that the factor α_2 appears in the $p = 2$ case is that for p an odd prime $S_{j,k}^p = S_{0,0}$, however, $(\alpha_2(1,1)S_{1,1})^2 = S_{0,0}$ since $S_{1,1}^2 = -S_{0,0}$.

IV. MUTUALLY UNBIASED BASES I

We review the theory of mutually unbiased bases (MUB) for a particle whose state vectors lie in a p-dimensional complex Hilbert space H_p, where p is a prime. It can be shown that there exist $p+1$ orthonomal bases (ONB) in this space which are MUB [11, 20, 29]; that is, if ψ and ϕ are state vectors that belong to a pair of ONB that are mutually unbiased, then $|\langle\phi|\psi\rangle| = 1/\sqrt{p}$. The simplest example of mutually unbiased bases occurs for $p = 2$, for which the bases are composed of the eigenvectors of the three Pauli matrices $\{\sigma_x, \sigma_y, \sigma_z\}$.

There is a nice way to characterize the MUB using commuting classes of the generalized spin matrices [1]. This leads to a natural way to introduce discrete phase space, and, in turn, to a definition of a Wigner function. We denote the two dimensional vector space with components in Z_p by $V_2(p)$, and use the letters u and v to denote vectors in this space. This vector space contains p^2 distinct points, and it is convenient to index the p^2 spin matrices using $V_2(p)$,

$$v = (v_0, v_1) \rightarrow S_v = S_{v_0, v_1}. \tag{16}$$

With this notation Eq. (13) becomes

$$S_u S_v S_u^\dagger = \eta^{u \circ v} S_v. \tag{17}$$

It follows from this that two spin matrices commute if and only if the symplectic inner product of their *index vectors* vanish. Therefore, the problem of finding commuting sets of operators is transformed into finding solutions to the equation $u \circ v = 0$ for vectors in the two dimensional vector space $V_2(p)$. The solutions are easy to find; the $p+1$ index vectors u_a, $a \in I_p = \{0, 1, \cdots, p\}$ partition the spin matrices into $p+1$ sets defined by

$$\begin{aligned}
C_a &= \{bu_a = b(1, a), \ b \in Z_p\} \rightarrow \mathfrak{M}_a = \{S_{u_a}^b, \ b \in Z_p\} \qquad a < p \\
C_p &= \{bu_p = b(0, 1), \ b \in Z_p\} \rightarrow \mathfrak{M}_p = \{S_{u_p}^b, \ b \in Z_p\}.
\end{aligned} \tag{18}$$

(Note: in [20] C_p was denoted by C_∞).

Equation (18) relates each vector in $V_2(p)$ to commuting sets of unitary matrices such that $\mathfrak{M}_a \cap \mathfrak{M}_b = \{S_{0,0}\}$ for $a \neq b$. This follows from the fact that in $V_2(p)$ two non-zero vectors with vanishing symplectic product must be collinear. The state vectors in each basis are the eigenvectors of the associated set of unitary matrices in Eq. (18). The projection operators for these vectors are defined in Eq. (15) and can be found in [1].
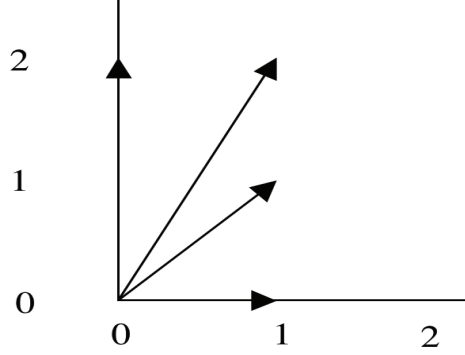
FIG. 1: The vectors u_a in $V_2(3)$.

$V_2(p)$ will be used as the phase space for a single system with Hilbert space H_p, and vectors in $V_2(p)$ will be used as indices for the characteristic function and for the Wigner function. The "horizontal" and "vertical" axes of $V_2(p)$ are associated with the spin matrices S_{u_0} and S_{u_p}, respectively. In general, a vector (or point) (j, k) in $V_2(p)$ corresponds to $S_{j,k}$. The projectors generated by S_{u_0} are associated with the basis is $\{|j\rangle,\ j \in Z_p\}$, and the projectors generated by S_{u_p} are associated with the basis $\{|k) = (1/\sqrt{p}) \sum_{j=0}^{p-1} \eta^{kj}|j\rangle,\ k \in Z_p\}$. The latter states are often referred to as the phase states, [23, 24, 27]. The Hermitian operators $J = \sum_{j=0}^{p-1} j|j\rangle\langle j|$ with eigenstates $\{|j\rangle\}$ and $\Phi = \sum_{k=0}^{p-1} k|k)(k|$ with eigenstates $\{|k)\}$ are said to be conjugate observables, since these states are Fourier transforms of one another. This is in analogy with the operators Q and P of section II although the commutation relation of J and Φ is not proportional to the identity operator, and is, therefore, state dependent.

The fact that the sets C_a correspond to a set of MUB can be seen by computing the projection operators for the sets, and showing that [20]

$$\sum_{r \in Z_p} P_{u_a}(r) = S_{0,0} \tag{19}$$

$$tr\left[P_{u_a}(r)P_{u_a}(s)\right] = \delta(r, s) \tag{20}$$

$$tr\left[P_{u_a}(r)P_{u_b}(s)\right] = \frac{1}{p} \quad \text{for } a \neq b. \tag{21}$$

In particular, the proof of Eq. (21) depends on the orthogonality of the spin matrices and

the fact that $tr(S_{j,k}) = 0$ for all the spin matrices except the identity. This set of MUB is complete in the sense that there are $p + 1$ ONB in the set, the maximum number possible [1].

V.   THE DISCRETE WIGNER FUNCTION FOR A SINGLE PARTICLE

A.   The Wigner function

The discrete Wigner function of interest here was introduced by Wootters in [28]. Following Wootters we wish to define the discrete analog of the Wigner function such that properties $1 - 5$ of section II are preserved. Our approach differs by emphasizing the role of the spin matrices.

Let p be a prime number, and $\rho \in M_p$ be a density matrix describing the state of a system on the Hilbert space H_p. Define the *characteristic function* over $V_2(p)$

$$\chi_\rho(mu_a) = \chi(mu_a) = tr\left[\rho\left(\alpha_p(u_a)S_{u_a}\right)^m\right], \tag{22}$$

where $\alpha_p(u)$ is defined above Eq. (15). The properties of χ that we shall need are

$$\chi(0) = 1 \tag{23}$$

$$\chi(mu_a)^* = \chi(-mu_a) \tag{24}$$

This last result follows from the fact that $(S_u^m)^\dagger = S_u^{-m}$, since S_u is unitary.

Let $v = (v_0, v_1)$ and $u = (u_0, u_1)$ be vectors in $V_2(p)$. Then using Eq. (11) the *discrete Wigner function* is defined as the discrete symplectic Fourier transform of the characteristic function:

$$
\begin{aligned}
W_\rho(v) = W(v) &= \frac{1}{p^2} \sum_{u \in V_2(p)} \eta^{v \circ u} \chi(u) \\
&= \frac{1}{p^2}\left(\chi(0) + \sum_{a=0}^{p}\sum_{m=1}^{p-1} \eta^{v \circ mu_a}\chi(mu_a)\right).
\end{aligned} \tag{25}
$$

The sum over m excludes the $m = 0$ term, which gives rise to the first term in brackets. The equality of these two expressions follows from the fact that the vectors $\{mu_a,\ a \in I_p,$ $m \in Z_p^*\} \cup \{(0,0)\} = V_2(p)$, where $Z_p^* = Z_p - \{0\}$, that is, these vectors partition the space into distinct lines through the origin. This fact illustrates the role of the geometry of $V_2(p)$, see appendix X E.

9

If we substitute Eq. (22) into (25) and use (15), the Wigner function can also be written as

$$W(v) = \frac{1}{p}\left(-1 + \sum_{a=0}^{p} tr\left[\rho P_{u_a}\left(v \circ u_a\right)\right]\right)$$

(26)

where $\{pr(r|a,\rho) = Tr\left[\rho P_{u_a}(r)\right], \ r \in Z_p\}$ is the probability distribution that can be estimated from one of the $p+1$ experiments determined by the set of MUB [20]. The sum over a gives a complete set of measurements for determining the Wigner function or, equivalently, as we shall see, the density matrix. This form of W shows that it is real and that it may be negative.

Equation (26) can be rewritten as

$$\begin{aligned} W(v) &= tr\left[\rho A(v)\right] \\ A(v) &= \frac{1}{p}\left(\sum_{a=0}^{p} P_{u_a}\left(v \circ u_a\right) - S_{0,0}\right). \end{aligned}$$

(27)

The set of Hermitian operators $\{A(v), \ v \in V_2(p^2)\}$ was used by Wootters in [8] to define the Wigner function and is an orthogonal basis of M_p. To verify this, one uses the MUB properties from Eq. (21) and computes as in [8]

$$Tr\left[A\left(u\right)A\left(v\right)\right] = \frac{1}{p^2}\left[p - 2\left(p+1\right) + \sum_a \sum_b Tr\left[P_{u_a}\left(u \circ u_a\right)P_{u_b}\left(v \circ u_b\right)\right]\right].$$

Regardless of u and v each term in the double sum equals $1/p$ when $a \neq b$. If $a = b$ and $u = v$, each of the resulting $p + 1$ terms equals 1. If $a = b$ and $u \neq v$, then the trace equals zero except for the one case when $u - v = mu_a$ so that $u \circ u_a = v \circ u_a$ and the trace equals one. Collecting terms gives

$$Tr\left[A\left(u\right)A\left(v\right)\right] = \frac{1}{p}\delta\left(u,v\right).$$

(28)

Note, by the way, that one can use the orthogonality to express the identity as

$$I = \sum_u A\left(u\right).$$

(29)

In the preceding discussion we have written *the* Wigner function and *the* characteristic function. In fact, for a given density matrix and a complete set of MUB, a class of Wigner and characteristic functions can be defined. For example we can multiply the characteristic funtion in Eq. (22) by an appropriate phase factor and get a new characteristic function

$$\chi_\rho(mu_a) \to \chi_{\rho,r_a}(mu_a) = \eta^{mr_a}\chi_\rho(mu_a),$$

where $r_a \in Z_p$. Under this transformation

$$W_\rho(v) \to W_{\rho,\mathbf{r}}(v) = \frac{1}{p}\left(-1 + \sum_{a=0}^{p} tr\left[\rho P_{u_a}\left(v \circ u_a + r_a\right)\right]\right),$$

where $\mathbf{r} = (r_0, \ldots, r_p)$. This approach provides an operational way of defining the class of Wigner functions described in [8] and in the recent work of [7].

Before showing that the definition Eq. (25) has the desired properties, we present three examples.

B. Examples

1. Qubits (p=2)

Using Eq. (8), the spin matrices may be shown to be equivalent to the Pauli matrices:

$$\begin{pmatrix} S_{0,0} & S_{0,1} \\ S_{1,0} & S_{1,1} \end{pmatrix} = \begin{pmatrix} \sigma_0 & \sigma_x \\ \sigma_z & i\sigma_y \end{pmatrix},$$

where σ_0 is the 2×2 identity. The classes of MUB are generated by

$$\begin{aligned} C_0 &= \{b(1,0)\} \to \{\sigma_0, \sigma_z\} \\ C_1 &= \{b(1,1)\} \to \{\sigma_0, i\sigma_y\} \\ C_2 &= \{b(0,1)\} \to \{\sigma_0, \sigma_x\} \end{aligned}$$

where $b \in Z_2$. The most general density matrix may be written as

$$\rho = \frac{1}{2}\left(\sigma_0 + \sum_j m_j \sigma_j\right)$$

where (m_x, m_y, m_z) is a vector with real components and length less than or equal to 1. In this case

$$\chi(u_0) = m_z, \ \chi(u_1) = m_y, \ \chi(u_2) = m_x.$$

We have included the factor $\alpha_2(u)$ so that χ is real. For $p = 2$ we have $\eta = -1$, and for $v = (v_0, v_1) \in V_2(2)$

$$W(v) = \frac{1}{4}\left(1 + m_z \eta^{v_1} + m_y \eta^{(v_1 - v_0)} + m_x \eta^{-v_0}\right).$$

11

It is now easy to see that summing over a horizontal line gives

$$\sum_{v_0=0}^{1} W(v) = \frac{1}{2}\left(1 + (-1)^{v_1}m_z\right) = tr\left[\rho P_{u_0}(v_1)\right],$$

$$P_{u_0}(0) = \frac{1}{2}(\sigma_0 + \sigma_z), \quad P_{u_0}(1) = \frac{1}{2}(\sigma_0 - \sigma_z),$$

where $P_{u_0}(0)$ is the projection operator for the state polarized along the positive z-axis, and $P_{u_0}(1)$ is the projection for the state polarized along the negative z-axis. A similar result holds for the sum over a vertical line, that is, a sum over v_1 and the x -axis. For $s \in Z_2$,

$$\sum_{v} W(v)\delta(v \circ u_2 - s, 0) = tr\left[\rho P_{u_1}(s)\right]$$

$$= \frac{1}{2}\left(1 + (-1)^s m_y\right)$$

which corresponds to summing along the line $\{b(1,1), \ b \in Z_2\}$. Finally, for this case, the Hermitian matrices defined in Eq. (27) are

$$A(v) = \frac{1}{4}\left(\sigma_0 + \sigma_z \eta^{v_1} + \sigma_y \eta^{(v_1-v_0)} + \sigma_x \eta^{-v_0}\right).$$

It is well-known that for a single particle $W(v)$ can serve as a hidden variable probablility distribution if it is nonnegative. This is because, as we shall see below, the measurement of an arbitrary observable O is given by

$$tr(\rho O) = p \sum_{v \in V_2(p)} W(v)W_O(v),$$

where $W_O(v)$ is the Wigner function defined with ρ replaced by O in Eq. (22). Therefore, if the Wigner function is non-negative we can construct a complete hidden variable theory of a single qubit consistent with quantum mechanics. However, there appear to be cases where this does not work, for our present example if $\mathbf{m} = (1,1,1)/\sqrt{3}$, then $W(0,0) < 0$ [8], see however [3] where it is shown that a hidden variable theory can always be constructed for a single spin. We also note that since this $\mathbf{m}$ corresponds to a pure state there are bases in which $W(v) \geq 0$. The positivity of the Wigner function is therefore sufficient but not necessary for the existence of a hidden variable theory. For a discussion of the positivity of the Wigner function see [7].

2. A pure state in H_p $(p > 2)$

Let $\rho = P_{u_b}(r)$, then for $a \in I_p$

$$
\begin{aligned}
\chi(mu_a) &= \frac{1}{p} \sum_{k=0}^{p-1} \eta^{-kr} tr\left(S_{u_a}^m \left(S_{u_b}^\dagger\right)^k\right) \\
&= \frac{1}{p} \sum_{k=0}^{p-1} \eta^{-kr} p\delta(a,b)\delta(m,k) \\
&= \delta(a,b)\eta^{-rm}.
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
W(v) &= \frac{1}{p^2}\left(1 + \sum_{m=1}^{p-1} \eta^{-m(r+u_{a1}v_0 - u_{a0}v_1)}\right) \\
&= \frac{1}{p}\delta\left(r + u_a \circ v, 0\right),
\end{aligned}
$$

so that $W(v)$ vanishes except at points along a line in $V_2(p)$. In particular for the case $a = p$, $W(v)$ vanishes everywhere except along the vertical line $v_0 = $ constant, and for $a = 0$, $W(v)$ is constant along the horizontal line $v_1 = $ constant and vanishes everywhere else.

Given an arbitrary pure state, we can always find a MUB that contains this state as one of the basis vectors. This shows that there is always a MUB for which a pure state has a non-negative Wigner function. On the other hand if the pure state is not chosen as one of the MUB vectors the result is more complicated as will be seen in example 4 below.

3. Completely random state

The density matrix for the completely random state is $\rho = (1/p)\mathbf{1}_p$, which gives $W(v) = 1/p^2$, that is, $W(v)$ is constant.

4. The operator $O = |j\rangle\langle k|$

As stated above, we can define a Wigner function for operators other than density matrices. We give an example here which we shall use later. For the case that p is an odd prime, let $|j\rangle$ and $|k\rangle$ be vectors in the standard basis and let

$$
O = |j\rangle\langle k|.
$$

Then for $a < p$

$$\chi_{j,k}(mu_a) = Tr\left[|j\rangle\langle k|(S_{u_a})^m\right],$$

and, for reasons that are explained in Section VII, we introduce a phase factor when a=p

$$\chi_{j,k}(mu_p) = Tr\left[|j\rangle\langle k|\left(\eta^{-2^{-1}}S_{u_p}\right)^m\right],$$

where -2^{-1} is taken as $(p-1)/2$ since in the exponent we can compute mod$p$. Using Eqs. (8) and (12), we find

$$\chi_{j,k}(mu_a) = \eta^{mk+a(m(m-1)/2)}\delta(j, ma+k),$$
$$\chi_{j,k}(mu_p) = \eta^{2^{-1}(k-j)}\delta(j, m+k).$$

Working through the details gives

$$W_{|j\rangle\langle k|}(v) = \frac{1}{p}\eta^{\left(v_0+2^{-1}\right)(k-j)}\delta\left(0, v_1 + 2^{-1}(j+k)\right), \qquad (30)$$

where $v = (v_0, v_1)$. Note that if $k = j$, $|j\rangle\langle j|$ is a density and $W_{|j\rangle\langle j|}$ is a special case of example 2 above. For $j \neq k$, we get

$$W_O(v)^* = W_{O^\dagger}(v).$$

Now suppose that $|\psi\rangle = \sum_{j=0}^{p-1} c_j|j\rangle$, then

$$W_{|\psi\rangle\langle\psi|}(v) = \frac{1}{p}\sum_{r=0}^{p-1}\eta^{(v_0+2^{-1})r}c_{-v_1-2^{-1}r}c^*_{-v_1+2^{-1}r}.$$

As stated above this is a more complicated form than we found for the case $|\psi\rangle\langle\psi| = P_b(r)$. For the case $p = 3$ we illustrate this in Fig. 2 for the case $|\psi\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$.

C. Properties of the Discrete Wigner Function

We now examine whether the definition (25) or, equivalently, (26) satisfies the criteria that we set out in part 1.

1. The mapping is $\rho \to W_\rho$ is linear on M_d and convex linear on the density matrices.
2. $W(v)$ is normalized since

$$\sum_{v_0 v_1=0}^{p-1} W(v) = \frac{1}{p^2}\left(p^2 + \sum_{a=0}^{p}\sum_{m=1}^{p-1}\chi(mu_a)p^2\delta(m,0)\right) = 1.$$

14

	0	1	2
2	1/6	1/6	1/6
1	1/6	1/6	1/6
0	-1/6	1/3	-1/6

FIG. 2: The Wigner function for $p = 3$ for the pure state $|\psi\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$.

3. The reality of W follows immediately from Eq. (26).

The first three results also follow directly from Eqs. (27) and (29).

4. For $w \in V_2(p)$, if $\rho' = S_w^\dagger \rho S_w$ then using Eq. (17)

$$\chi_{\rho'}(u) = \eta^{w \circ u} \chi_\rho(u)$$
$$W_{\rho'}(v) = W_\rho(v + w).$$

Note that if ρ commutes with S_w, the Wigner function is invariant under translations along w. Furthermore, the characteristic function vanishes for u such that $w \circ u \neq 0 \mod p$.

5. The marginal distributions are easily computed. We consider the more general case of summing along the points on any of the lines in phase space, where a line in phase space $V_2(p)$ is defined as the set of points that satisfy the equation

$$L(b, s) = \{(x, y) : -xb + y - s = (x, y) \circ u_b - s = 0, \quad b, s \in Z_p\}$$
$$L(p, s) = \{(s, y) : -x + s = (x, y) \circ u_p + s = 0, \quad b, s \in Z_p\}. \tag{31}$$

$L(b, s)$ is the line with "slope" b which intersects the vertical axis at s, and $L(p, s)$ is a

"vertical" line that intersects the horizontal axis at $x = s$ (see Appendix X E). Let

$$f_b(s) = \sum_v W(v)\delta(v \circ u_b - s, 0),$$

then using Eqs. (26) and (21), we can show that

$$
\begin{aligned}
f_b(s) &= \frac{1}{p}\left(-p + \sum_{a \neq b} tr\left[\rho \sum_{r=0}^{p-1} P_{u_a}(r)\right] + p\ tr\ [\rho P_{u_b}(s)]\right) \\
&= tr\ [\rho P_{u_b}(s)].
\end{aligned}
$$

We have used the fact that for $a \neq b$ the sum over v becomes a sum over Z_p, and this sum is the identity operator, while for $a = b$, we have $v \circ u_b = s$. Therefore, we see that summing the Wigner function over any line in phase space gives the probablilty that the system is in the corresponding MUB state.

6. Since W_ρ and χ_ρ are Fourier transforms of one another, Plancheral's formula gives

$$p^2 \sum_v W_\rho(v)^2 = |\chi_\rho(0)|^2 + \sum_{a=0}^{p}\sum_{m=1}^{p-1} |\chi_\rho(mu_a)|^2. \tag{32}$$

We also have, setting $mu_a = (j, k) = v$,

$$|\chi_\rho(v)|^2 = |tr\rho S_v|^2 = \langle \rho, S_v \rangle \langle S_v, \rho \rangle.$$

using Eq. (7). More generally,

$$\chi^*_{\rho_1}(v)\chi_{\rho_2}(v) = (tr\rho_1 S_v)^*\ tr\rho_2 S_v = \langle \rho_1, S_v \rangle \langle S_v, \rho_2 \rangle.$$

Summing over the complete set of S_v, from Eq. (14), we can write Plancheral's formula,

$$tr\ [\rho_1\rho_2] = p \sum_v W_{\rho_1}(v)W_{\rho_2}(v). \tag{33}$$

See also [8] where the derivation is based on Eq. (28).

The support of a function $f(v)$ on phase space is defined by

$$supp(f) = \{v \in V_2(p):\ f(v) \neq 0\} \tag{34}$$

and $|supp(f)|$ is defined as the number of points in $supp(f)$. From Eq. (33) we have

$$pW_\rho^2(v_0) \leq p \sum_v W_\rho^2(v) = tr\rho^2 \leq 1. \tag{35}$$

16

which implies that for any point v_0,

$$|W(v_0)| \leq \frac{1}{\sqrt{p}}.$$

Now let

$$\mu_{W_\rho}(v) = \begin{cases} 1 & v \in suppW_\rho \\ 0 & \text{otherwise.} \end{cases}$$

Then applying the Schwarz inequality to the normalization equation and using Eq. (35) we get

$$1 = \sum_v W_\rho(v)\mu_{W_\rho}(v) \leq \sqrt{\sum_v W_\rho^2(v)\mu_{W_\rho}(v) \sum_u \mu_{W_\rho}(u)} \leq \sqrt{\frac{1}{p}|suppW_\rho|}$$

or

$$|suppW_\rho| \geq p.$$

This is analogous to the continuous case where the uncertainty principle implies that $W(q, p)$ can not be concentrated into too small a region. We have seen that if ρ is a pure state selected from the MUB that $|suppW_\rho| = p$, and $W_\rho(v) = 1/p$ on its support, so the lower bound is attained.

If ρ_1 and ρ_2 correspond to orthogonal states, then Eq. (33) gives

$$\sum_v W_{\rho_1}(v)W_{\rho_2}(v) = 0,$$

which along with the normalization condition implies that, either $suppW_{\rho_1}$ and $suppW_{\rho_2}$ are disjoint or at least one of the Wigner functions must take on negative values. For example, we saw in V B 2 that the orthogonal states in one of the bases of a set of MUB have support on non-intersecting lines of $V_2(p)$.

There is an inequality, referred to as an uncertainty principle, that also follows from the discrete Fourier transform:

$$|suppW_\rho|\,|supp\chi_\rho| \geq p^2,$$

[22]. Equality holds for the random state discussed in example V B 3 above.

D. Inversion formula

In the case of continuous phase space, the density matrix for a particle confined to one-dimension can be obtained from Eq. (6) by using the inverse Fourier integral. We can

17

proceed in a similar manner for the discrete case. First using the discrete Fourier inversion formula,

$$\chi(mu_a) = \sum_{v \in V(p^2)} W(v)\eta^{-v \circ mu_a} \tag{36}$$

Then from Eq. (22) and the completeness of the spin matrices

$$\rho = \frac{1}{p}\left(S_{0,0} + \sum_{a=0}^{p}\sum_{m=1}^{p-1}\chi(mu_a)^* S_{u_a}^m\right). \tag{37}$$

Substituting (36) into (37), and using Eqs. (15) and (27), we also get

$$\rho = \sum_{v \in V(p^2)} W(v)A(v). \tag{38}$$

Therefore, we have an expression for the density matrix as an expansion in the spin matrices with coefficients given by the characteristic function and an equivalent expansion in terms of a basis of Hermitian operators with the Wigner function as coefficients.

VI.   MUTUALLY UNBIASED BASES II

To define the generalized spin matrices in the case when $d = p^n$ where p is prime, we require the notion of a finite or Galois field $GF(p^n)$, see Appendices X A and X B for more details. There is a systematic way of representing the elements in $GF(p^n)$ that uses the structure of polynomials irreducible over $GF(p) = Z_p$. An irreducible polynomial is a polynomial $f(x)$ of degree n with coefficients in $GF(p)$ that can not be factored into non-constant polynomials of lower degree. Then the elements of $GF(p^n)$ may be represented by polynomials of degree less than n with coefficients in $GF(p)$. The simplest example is that of two qubits, $p = 2$, $n = 2$. In this case the irreducible polynomial is unique and is given by $x^2 + x + 1$. Define λ to be a symbolic solution of $x^2 + x + 1 = 0 \mod 2$. Then every element of $GF(2^2)$ can be written as $\alpha = a_0 + \lambda a_1$ where a_0 and a_1 are in $GF(2)$. This is analogous when working with real numbers to letting i denote a symbolic solution of the equation $x^2 + 1 = 0$ and introducing complex numbers as $x + iy$.

For the case of $n = 2$ and p an odd prime, let D be an element in $GF(p^2)$ such that there is no solution in $Z_p = GF(p)$ to the equation $x^2 - D = 0 \mod p$. In technical terms, D is a *quadratic non-residue* of p. There are an equal number of *quadratic residues* and quadratic non-residues in $GF(p)$. Then elements in $GF(p^2)$ can be represented as $j + k\lambda$, where j and

18

k are in $GF(p)$ and λ is taken to be a symbolic solution of $x^2 - D = 0 \bmod p$. Addition and multiplication of elements of $GF(p^2)$ are defined by

$$(j_1 + k_1\lambda) + (j_2 + k_2\lambda) = (j_1 + j_2) + (k_1 + k_2)\lambda$$
$$(j_1 + k_1\lambda)(j_2 + k_2\lambda) = (j_1 j_2 + Dk_1 k_2) + (j_1 k_2 + k_1 j_2)\lambda,$$

where the additions in the parentheses are modulo p. We refer to Appendix X B for more details.

We can construct a complete set of mutually unbiased bases when $d = p^n$ by following the same procedure that was used in the $d = p$ case [28]. The key idea for constructing a MUB is based on the fact that we can define a two-dimensional vector space $V_2(p^n)$ over $GF(p^n)$, and $p^n + 1$ generating vectors u_α where α is in the index set $I_{p^n} = GF(p^n) \cup \{p^n\}$. Specifically, define

$$u_\alpha = \begin{cases} (1, \alpha), & \alpha \in GF(p^n) \\ (0, 1), & \alpha = p^n \end{cases} \tag{39}$$

Each of these vectors can be used to define a class containing p^n vectors,

$$C_\alpha = \{\beta u_\alpha, \beta \in GF(p^n)\} \tag{40}$$

where $\alpha \in I_{p^n}$. Each pair of vectors in a class has vanishing symplectic product, Eq. (11) where the operations are with respect to $GF(p^n)$. We want to find a spin matrix representation of these classes, that is, we wish to find a mapping from this space to the set of tensor products

$$S_{\mathbf{u}} = \bigotimes_{r=0}^{n-1} S_{u_r} \tag{41}$$

where $\mathbf{u} = \bigoplus_{r=0}^{n-1} u^{(r)} \in V_{2n}(p)$ and each $u^{(r)} \in V_2^{(r)}(p) = V_2(p)$. To do this we define an isomorphism

$$M : V_2(p^n) \to V_{2n}(p) = \bigoplus_{j=0}^{n-1} V_2^{(j)}(p)$$

that preserves the symplectic product in the following sense. For each vector $v \in V_2(p^n)$, if $M(v) = \mathbf{v} = \bigoplus_{j=0}^{n-1} u^{(j)}$, where $u^{(j)} \epsilon V_2^{(j)}(p)$, define

$$\mathbf{v}_1 \circ \mathbf{v}_2 = \sum_{j=0}^{p-1} (u_1^{(j)} \circ u_2^{(j)}). \tag{42}$$

Then $v_1 \circ v_2 = 0$ implies $\mathbf{v}_1 \circ \mathbf{v}_2 = 0$ as is shown in Eq. (87). We present an outline of the derivation of M in Appendix X B and refer to [20] for another discussion. It is worth noting that the construction of $V_{2n}(p)$ is analogous to what is done in the continuous case. There we take the direct sum of the two-dimensional vector spaces corresponding to independent conjugate position and momentum pairs.

To perform the analog of what was done in Eq. (18), it is useful to introduce the generators of the index set for the set of MUB, again the details are given in Appendix X B. For $\alpha \in I_{p^n}$, define $\lambda^r u_\alpha \in V_2(p^n)$, $r = 0, \cdots, n-1$. Then define a set of generators on $V_{2n}(p)$

$$G_\alpha = \{\mathbf{g}_r(\alpha) = M\left(\lambda^r u_\alpha\right), \ r = 0, \cdots, n-1\}, \tag{43}$$

and define the corresponding spin matrix using Eq. (41) as

$$S^b_{\mathbf{g}_r(\alpha)} \equiv \bigotimes_{j=0}^{n-1} S^b_{u_r^{(j)}(\alpha)} \tag{44}$$

where each $S_{u^{(j)}}$ acts on a Hilbert space H_p. The generalization of Eq. (18) is

$$G_\alpha \to \mathfrak{M}_\alpha = \left\{ \prod_{r=0}^{n-1} S^{b_r}_{\mathbf{g}_r(\alpha)} = \bigotimes_{j=0}^{n-1} \prod_{r=0}^{n-1} S^{b_r}_{u_r^{(j)}(\alpha)}, \quad b_r \in GF(p) \right\} \tag{45}$$

for the generation of $p^n + 1$ disjoint sets of p^n of commuting operators $\mathfrak{M}_\alpha$ where $\mathfrak{M}_\alpha \cap \mathfrak{M}_\beta = \{S_{0,0}\}$ for all $\alpha \neq \beta$. We have written the mapping in Eq. (45) from the set of basis vectors G_α rather than the space C_α.

It is also possible to write down the set $\{P_\alpha(r), r \in V_n(p)\}$ of rank one orthogonal projections defined by each of the $p^n + 1$ commuting classes $\mathfrak{M}_\alpha$. This gives the set of MUB as projections defined explicitly in terms of sums of the spin matrices in each class. The procedure to do this is discussed in [20], and is illustrated there for the case for $n = 2$. The corresponding projection operators for the case $p > 2$ are

$$P_\alpha(\mathbf{s}) = \prod_{r=0}^{n-1} P_{\mathbf{g}_r(\alpha)}(s_r)$$

$$P_{\mathbf{g}_r(\alpha)}(s_r) = \left(\frac{1}{p} \sum_{b_r=0}^{p-1} \left[\eta^{s_r} S_{\mathbf{g}_r(\alpha)} \right]^{b_r} \right), \tag{46}$$

where $\mathbf{s} = (s_0, \ldots, s_{n-1})$. For $p = 2$ it is necessary to include the factors $\alpha_2(j, k)$ in the definition of the projection operators as shown in Eq. (15). $P_\alpha(\mathbf{r})$ has trace one, and it is straightforward to check that if $\mathbf{r} \neq \mathbf{s}$

$$P_\alpha(\mathbf{r}) P_\alpha(\mathbf{s}) = \delta(\mathbf{r}, \mathbf{s}) P_\alpha(\mathbf{r}).$$

It is easy to show that each $P_\alpha(\mathbf{r})$ is a product of commuting projections. One can also show that $P_\alpha(\mathbf{r}) = (P_\alpha(\mathbf{r}))^\dagger$, and it follows that $P_\alpha(\mathbf{r})$ is a rank one orthogonal projection and that

$$I = \sum_\mathbf{r} P_\alpha(\mathbf{r}).$$

Finally, it can be shown that for $\alpha \neq \beta$ that

$$tr\left[P_\alpha(\mathbf{r})P_\beta(\mathbf{s})\right] = \frac{1}{1/p^n}.$$

The explicit calculation of the projections and of the set of vectors in $V_{2n}(p)$ corresponding to C_α depends quite specifically on p and n and on the representation of elements in the different finite fields. When $n = 2$ and p is an odd prime, however, one can give a unified summary of the results of the theory. Without going through the detailed construction outlined in Appendix X B, it is easy to check that the vectors in each of the classes below have symplectic product zero.

Example $d=p^2$

Let $d = p^2$ with p an odd prime and D such that $x^2 - D = 0 \bmod p$ has no solution in $GF(p)$. In Appendix X B, Eq. (92) it is shown that the $p^2 + 1$ commuting classes of indices are generated by

$$G_{a_0,a_1} = \{(1, 2a_0, 0, 2Da_1), (0, 2Da_1, 1, 2Da_0))\}$$

where a_0 and a_1 are in $GF(p)$, and

$$G_{p^2} = \{(0, 1, 0, 0), (0, 0, 0, 1))\}.$$

One can check directly that the vectors in each G_{a_0,a_1} have vanishing symplectic product. Then the spin matrices that generate the commuting classes may be written as

$$G_{a_0,a_1} \rightarrow \mathfrak{M}_{(a_0,a_1)} = \left\{ (S_{1,2a_0} \otimes S_{0,2Da_1})^{b_0} (S_{0,2Da_1} \otimes S_{1,2Da_0})^{b_1}, \ b_0, b_1 \in GF(p) \right\},$$
$$G_{p^2} \rightarrow \mathfrak{M}_{p^2} = \left\{ (S_{0,1}^{b_0} \otimes S_{0,0}) (S_{0,0} \otimes S_{0,1}^{b_1}), \ b_0, b_1 \in GF(p) \right\}. \tag{47}$$

The corresponding projections are given by

$$P_{a_0,a_1}((r_0,r_1)) = \frac{1}{p} \sum_{b_0=0}^{p-1} \left((\eta^{r_0} S_{1,2a_0} \otimes S_{0,2Da_1})^{b_0} \right) \frac{1}{p} \sum_{b_1=0}^{p-1} \left((\eta^{r_1} S_{0,2Da_1} \otimes S_{1,2Da_0})^{b_1} \right)$$
$$P_{p^2}((r_0,r_1)) = \frac{1}{p} \sum_{b_0=0}^{p-1} \left((\eta^{r_0} S_{0,1} \otimes S_{0,0})^{b_0} \right) \frac{1}{p} \sum_{b_1=0}^{p-1} \left((\eta^{r_1} S_{0,0} \otimes S_{0,1})^{b_1} \right).$$

We note that each of these one-dimensional projection operators is the product of two commuting rank p-dimenional projections. The two p-dimensional spaces that they project onto intersect in a one-dimensional space.

VII. WIGNER FUNCTION FOR $d = p^2$

In earlier work [2, 8], the phase space on which the Wigner functions were defined when $d = p^n$ was chosen to be $V_2(p^n)$. The advantage of this choice is that one can use the underlying geometry to great advantage. The disadvantage is that one has to label coordinates using elements from the Galois field $GF(p^n)$ which does not lend itself to a discussion of separability. However, as we saw in Section VI, and as is elaborated in Appendix XB, there is a natural isomorphism M between $V_2(p^n)$ and $V_{2n}(p)$ which encodes the geometry of $V_2(p^n)$ in $V_{2n}(p)$. We take advantage of this structure to define our Wigner function on $V_{2n}(p)$ This is in close analogy to the continuous case and simplifies computations involving the generalized spin matrices.

In particular, this approach enables questions involving separability to be treated efficiently. In this section we illustrate the ideas in detail for $n = 2$, leaving the generalizations to the next section and the Appendix.

A. Separability of the Wigner Function for p an odd prime

We consider a bipartite system composed of subsystems of dimension p, a prime. As we saw in Section 5, there is a certain latitude in the definition of the Wigner function that is available because of the freedom to include phase factors in the characteristic function. Our goal in this section is to show how that freedom enables us to define Wigner functions for one and two subsystems so that separability is respected. Specifically, for a product state we want

$$\rho = \tau \otimes \mu \Rightarrow W_\rho\left(\mathbf{u}\right) = W_\tau\left(u^{(0)}\right) W_\mu\left(u^{(1)}\right), \tag{48}$$

where $\mathbf{u} = u^{(0)} \oplus u^{(1)}$. Then, since $W_\rho\left(\mathbf{u}\right)$ is convex linear on the space of densities, we will have the general statement that

$$\rho = \sum_k p_k \tau_k \otimes \mu_k \Rightarrow W_\rho\left(\mathbf{u}\right) = \sum_k p_k W_{\tau_k}\left(u^{(0)}\right) W_{\mu_k}\left(u^{(1)}\right). \tag{49}$$

A natural definition of the characteristic function $\chi = \chi_\rho$ is to use Eq. (44) with $n = 2$, and define

$$\widetilde{\chi}(\mathbf{w}) = tr\left[\rho S_{\mathbf{g}_0(\alpha)}^{b_0} S_{\mathbf{g}_1(\alpha)}^{b_1}\right] \tag{50}$$

where $\mathbf{w} = b_0\mathbf{g}_0(\alpha) + b_1\mathbf{g}_1(\alpha)$. We can rewrite the product of the S matrices on H_{p^2} as a direct product of S matrices on $H_p^{(0)} \otimes H_p^{(1)}$. Rewriting $\mathbf{w} = u^{(0)} \oplus u^{(1)}$ where $u^{(j)} \in V_2^{(j)}(p)$, we find

$$\widetilde{\chi}(\mathbf{w}) = \eta^\Phi tr\left[\rho S_{u^{(0)}} \otimes S_{u^{(1)}}\right].$$

The problem with this definition is that in general $\Phi \neq \phi(u^{(0)}) + \phi(u^{(1)})$, so that the corresponding Wigner function would not factor when ρ is a product state. Now as pointed out before, there is some freedom in the choice of phase in defining the characteristic function and the Wigner function. For this reason it is convenient to introduce a phase factor into the definition of the characteristic function to avoid this problem. We shall therefore define the characteristic function as

$$\chi(\mathbf{w}) = \eta^{-\Theta}\widetilde{\chi}(\mathbf{w}), \tag{51}$$

using Eq. (50) and the Θ defined in Eq. (99) that is linear in b_0 and b_1. The linearity in the $b's$ is important, as we shall see, because we want to write the analog of Eq. (26) with the appropriate projection operators given in Eq. (46).

The underlying reason for having to introduce the phases arises from the fact that we are using the geometries of $V_2(p^2)$ and $V_4(p)$. That fact forces us to go into some detail to define appropriate phase factors and to confirm that they work.

For example, consider the case of p odd discussed at the end of the last section. For $\alpha \neq p^2$ define

$$\chi_\rho(\mathbf{w}) = Tr\left[\rho\left(\eta^{-Da_1}S_{\mathbf{g}_0}\right)^{b_0}\left(\eta^{-Da_1}S_{\mathbf{g}_1}\right)^{b_1}\right], \tag{52}$$

and for $\alpha = p^2$ define

$$\chi_\rho(\mathbf{w}) = Tr\left[\rho\left(\eta^{-2^{-1}}S_{\mathbf{g}_0}\right)^{b_0}\left(\eta^{-2^{-1}}S_{\mathbf{g}_1}\right)^{b_1}\right]. \tag{53}$$

Then define

$$W_\rho(\mathbf{u}) = \frac{1}{p^4}\sum_{\mathbf{w}}\eta^{\mathbf{u}\circ\mathbf{w}}\chi_\rho(\mathbf{w}). \tag{54}$$

Note again that -2^{-1} is computed modulo p and equals $(p-1)/2$. The vector symplectic product in the exponent of η is defined in Eq. (42). From Eq. (25) we can write out the right hand side of Eq. (48) with one modification. For $mu_p = m(0,1)$ take

$$\chi_\tau(mu_p) = tr\left[\tau\left(\eta^{-2^{-1}}S_{u_p}\right)^m\right],\tag{55}$$

as we did in Example 4 of Section V. Then $W_\tau(u)$ is defined as the usual symplectic tranform and can be written as

$$W_\tau(u) = \frac{1}{p^2}\left[\sum_{m=0}^{p-1}\eta^{u\circ mu_p}\chi_\tau(mu_p) + \sum_{c=0}^{p-1}\sum_{m=1}^{p-1}\eta^{u\circ mu_c}\chi_\tau(mu_c)\right].\tag{56}$$

Finally, we get the right hand side of Eq. (48) as the trace of $\frac{1}{p^2}(\tau\otimes\mu)$ times the expression

$$rhs = \sum_{m_0=0}^{p-1}\sum_{m_1=0}^{p-1}\eta^{\mathbf{u}\circ(0,m_0,0,m_1)}\eta^{-2^{-1}(m_0+m_1)}S_{m_0u_p}\otimes S_{m_1u_p} +$$

$$\sum_{(c_0,c_1)\neq(p,p)}\sum_{(m_0,m_1)\neq(0,0)}\eta^{\mathbf{u}\circ\left(m_0u_{c_0}\oplus m_1u_{c_1}\right)}\eta^{-2^{-1}(\delta(c_0,p)m_0+\delta(c_1,p)m_1)}\left(S_{u_{c_0}}\right)^{m_0}\otimes\left(S_{u_{c_1}}\right)^{m_1}.$$

The left hand side of Eq. (48) can be written as the trace of $\frac{1}{p^2}(\tau\otimes\mu)$ times the expression

$$lhs = \sum_{b_0=0}^{p-1}\sum_{b_1=0}^{p-1}\eta^{\mathbf{u}\circ\left(b_0\mathbf{g}_0(p^2)+b_1\mathbf{g}_1(p^2)\right)}\eta^{-2^{-1}(b_0+b_1)}S_{(0,b_0,0,b_1)} +$$

$$\sum_{\alpha\neq p^2}\sum_{(b_0,b_1)\neq(0,0)}\eta^{\mathbf{u}\circ(b_0\mathbf{g}_0(\alpha)+b_1\mathbf{g}_1(\alpha))}\eta^{-Da_1(b_0+b_1)}\left(S_{\mathbf{g}_0(\alpha)}\right)^{b_0}\left(S_{\mathbf{g}_1(\alpha)}\right)^{b_1}.$$

Note that in this equation we have the ordinary matrix product in the second term.

Our goal is to confirm that Eq. (48) holds with the above definitions of the characteristic functions. Using Eq. (12) we can pair the indices of the spin matrices in Eq. (48) to obtain the *index equation* relating terms in *rhs* to *lhs*,

$$\mathbf{w} = m_0u_{c_0}\oplus m_1u_{c_1} = b_0\mathbf{g}_0(\alpha) + b_1\mathbf{g}_1(\alpha),\tag{57}$$

which includes the $\mathbf{w} = (0,0,0,0)$ term that is incorporated in the first summations. It follows that the phase factor $\eta^{\mathbf{u}\circ(b_0\mathbf{g}_0(\alpha)+b_1\mathbf{g}_1(\alpha))}$ is common to the corresponding terms of *rhs* and *lhs*, and we can cancel it. It is also obvious that the $\alpha = p^2$ terms equal the corresponding terms associated with $c_0 = c_1 = p$ and that the remaining phase factors in this case are also equal if we set $m_k = b_k$.

24

To match terms in the second sets of summations, we multiply out the powers of the spin matrices in *lhs* to obtain

$$S_{m_0 u_{c_0}} \otimes S_{m_1 u_{c_1}} = S_{b_0(1,2a_0)+b_1(0,2Da_1)} \otimes S_{b_0(0,2Da_1)+b_1(1,2Da_0)},$$

where the equality follows from the index equation. This process introduces phase factors using Eqs.(10) and (12), and it remains to prove that the resulting exponents of η are equal. Specifically, one has to verify that subject to Eq. (57)

$$(1 - \delta(c_0, p)) c_0 \binom{m_0}{2} + (1 - \delta(c_1, p)) c_1 \binom{m_1}{2} - 2^{-1} (\delta(c_0, p) m_0 + \delta(c_1, p) m_1) \qquad (58)$$

equals

$$-Da_1(b_0 + b_1) + 2a_0 \binom{b_0}{2} + 2Da_0 \binom{b_1}{2} + 2b_0 b_1 Da_1. \qquad (59)$$

We verify the equality for $\alpha \neq p^2$ by considering different cases. Let $\alpha = a_0 + a_1 \lambda$. If b_0 and b_1 are both non-zero, $m_0 = b_0$, $m_1 = b_1$ and

$$
\begin{aligned}
b_0 c_0 &= b_0 2a_0 + b_1 2Da_1, \\
b_1 c_1 &= (b_0 2Da_1 + b_1 2Da_0).
\end{aligned}
$$

If $b_0 = 0$,

$$\mathbf{w} = (0, b_1 2Da_1) \oplus (b_1, b_1 2Da_0)$$

and $c_0 = p$, $m_0 = b_1 2Da_1$, $c_1 = 2Da_0$ and $m_1 = b_1$. Similarly, for $b_1 = 0$

$$\mathbf{w} = (b_0, b_0 2a_0) \oplus (0, b_0 2Da_1),$$

and $m_0 = 2Da_0$, $m_0 = b_0$, $m_0 = p$ and $m_1 = b_0 2Da_1$. Substituting these expressions in Eq. (58) gives (59). We have gone through this in some detail because the method illustrated generalizes to the case of complete separability of n subsystems. It should be noted that the argument leading to Eq. (48) did not require that τ or μ be a density matrix.

Our ability to add a phase factor to the definition of the characteristic function is related to an arbitrariness in the assigning of state vectors in a basis on the Hilbert space to lines in phase space as noted in [8]. This is illustrated in VII C 2 below.

A different definition of the Wigner function in terms of the characteristic function can be found in [24]. Vourdas replaces the M transformation by introducing the trace operation into the Fourier transformation.

B.   Properties of the Wigner Function

Because we have used the same format in defining the Wigner function for two subsystems, Eq. (54), as was used in defining it for a single subsystem, Eq. (25), we expect the properties in Section II to hold. With the definition of $\chi_\rho(\mathbf{w})$ in Eqs. (52) and (53) conditions (23) and (24) are satisfied. The discrete Wigner function W_ρ for a density ρ on H_{p^2} is defined using the symplectic Fourier transform Eq. (54); consequently, W_ρ is convex linear on the space of densities and linear on the space of $p^2 \times p^2$ matrices. Again, the defining Eq. (54) is invertible, so that one can obtain the $\chi_\rho(\mathbf{w})$ and thus the spin coefficients of ρ from the Wigner function. With this definition Plancheral's formula becomes

$$p^4 \sum_{\mathbf{v} \in V_4(p)} |W(\mathbf{v})|^2 = |\chi(0)|^2 + \sum_{q,r=0}^{p} \sum_M |\chi(m^{(0)} u_q^{(0)} \oplus m^{(1)} u_r^{(1)})|^2.$$

We also have, as in Eq. (33), that

$$tr[\rho_1 \rho_2] = p^2 \sum_{\mathbf{v}} W_{\rho_1}(\mathbf{v}) W_{\rho_2}(\mathbf{v}),$$

and, consequently, $|W(\mathbf{v})| \le 1/p$ and $|suppW(\mathbf{v})| \ge 1/p^2$. Using the notation of Eq. (46), we can write

$$W_\rho(\mathbf{u}) = tr[\rho A(\mathbf{u})] \tag{60}$$

where

$$\begin{aligned}
p^2 A(\mathbf{u}) &= -S_{0,0} \otimes S_{0,0} + P_{p^2}\left(-2^{-1} + \mathbf{u} \circ \mathbf{g}_0\left(p^2\right), -2^{-1} + \mathbf{u} \circ \mathbf{g}_1\left(p^2\right)\right) \tag{61} \\
&\quad + \sum_{\alpha \ne p^2} P_\alpha\left(-Da_1 + \mathbf{u} \circ \mathbf{g}_0(\alpha), -Da_1 + \mathbf{u} \circ \mathbf{g}_1(\alpha)\right),
\end{aligned}$$

corresponding to Eq. (27). From Eq. (61) it follows that W_ρ is real for densities ρ. In particular, $\{A(\mathbf{u})\}$ again defines a complete orthogonal set of Hermitian matrices. The argument is analogous to that leading to Eq. (27) and leads to

$$Tr[A(\mathbf{u}) A(\mathbf{v})] = p^{-2}\delta(\mathbf{u}, \mathbf{v})$$

Thus we can interpret the Wigner function W_ρ as the set of coefficients of ρ in the orthogonal expansion relative to $\{A(\mathbf{u})\}$ analogous to Eq. (38) .

The analogues of the other properties of Section V C follow in the same way as before. W is normalized since we can use Eq. (60) to prove

$$\sum_{\mathbf{u}} W_\rho(\mathbf{u}) = Tr\left[\rho \sum_{\mathbf{u}} A(\mathbf{u})\right] = Tr[\rho] = 1$$

26

since Eq. (29) holds in this case. If $\rho' = S_{\mathbf{z}}^\dagger \rho S_{\mathbf{z}} \in H_p \otimes H_p$, then $\chi_{\rho'}(\mathbf{w}) = \eta^{\mathbf{z} \circ \mathbf{w}} \chi_\rho(\mathbf{w})$, and $W_{\rho'}(\mathbf{u}) = W_\rho(\mathbf{u} + \mathbf{z})$ as before.

Summing $W_\rho(\mathbf{u})$ over a "line" in $V_2(p^2)$ corresponds to summing over a translation of a two dimensional subspace in $V_4(p)$ and again leads to a marginal probability $Tr[\rho P_\alpha(s_1, s_2)]$. To see this let C_α denote the two dimensional subspace associated with α. It is easy to show that

$$\sum_{\mathbf{u} \in C_\alpha} W_\rho(\mathbf{u} + \mathbf{r}) = \frac{1}{p^2} \sum_{\mathbf{w} \in C_\alpha} \eta^{\mathbf{r} \circ \mathbf{w}} \chi_\rho(\mathbf{w}).$$

This can be written as the trace of ρ against the projection $P_\alpha(s_1, s_2)$ for appropriate indices s_1 and s_2 which depend on $\mathbf{r}$ and the phase factors used in the definition of the characteristic functions. Thus using definition of Eq. (54) the Wigner function satisfies the conditions proved in section V C and the requirement that W_ρ factor for separable ρ as in Eq. (49).

As pointed out to us by Wootters, Eq. (48) may be used to give a positive answer to a question posed in [8]. That is, with the phase factors given above, we have

$$A(\mathbf{u}) = A(u^{(0)}) \otimes A(u^{(1)}).$$

where $\mathbf{u} = u^{(0)} \oplus u^{(1)}$. The proof is easy, rewrite Eq. (48) as

$$tr\left[\tau_0 \otimes \tau_1 A(\mathbf{u})\right] = tr\left[\tau_0 \otimes \tau_1 A(u^{(0)} \oplus A(u^{(1)}))\right].$$

This equality holds even the τ's are not densities. Since Hermitian matrices of the form $\tau \otimes \mu$ form a basis of M_{p^2}, this inequality holds for all $A(\mathbf{u})$ for all $\mathbf{u} \in V_4(p)$.

C. Examples

1. Maximally entangled state

For prime p let $|\Psi\rangle = \frac{1}{\sqrt{p}} \sum_j |j\rangle |j\rangle$, so that $\rho \equiv |\Psi\rangle \langle\Psi| = \frac{1}{p} \sum_{j,k} |j\rangle \langle k| \otimes |j\rangle \langle k|$. By the separability property and linearity we know that if $\mathbf{u} = u^{(0)} \oplus u^{(1)} = (x_0, y_0, x_1, y_1)$, then

$$W_\rho(\mathbf{u}) = \frac{1}{p} \sum_{j,k} W_{|j\rangle\langle k|}\left(u^{(0)}\right) W_{|j\rangle\langle k|}\left(u^{(1)}\right),$$

where $W_{|j\rangle\langle k|}(u)$ is defined in Eq. (30). It follows that

$$W_\rho(\mathbf{u}) = \frac{1}{p^3} \sum_{j,k} \eta^{(x_0 + x_1 + 1)(k-j)} \delta\left(y_0 + 2^{-1}(j+k), 0\right) \delta\left(y_0 + 2^{-1}(j+k), 0\right),$$

27

and simplifying we get

$$W_\rho(\mathbf{u}) = \frac{1}{p^2}\delta\left(1 + x_0 + x_1, 0\right)\delta\left(y_0, y_1\right)$$

Thus the Wigner function for this maximally entangled state equals $1/p^2$ for the p^2 four-vectors with $u^{(0)} = (x_0, y_0)$ and $u^{(1)} = (-1 - x_0, y_0)$ and equals zero elsewhere.

Although the Wigner function for this state is positive, it is a non-classical state. In particular, entangled states violate Bell inequalities. Since the Wigner function discussed in this example is not separable, it need not respect mathematical inequalities based on separability.

2. MUB

Let $\rho = P_\alpha\left(s_0, s_1\right)$. In this case it is simplest to use Eq. (61) so that

$$
\begin{aligned}
W_\rho(\mathbf{u}) &= \frac{1}{p^2}tr\left[P_\alpha\left(s_0, s_1\right)A(\mathbf{u})\right] \\
&= \frac{1}{p^2}\left[-1 + \sum_{\beta\neq\alpha}Tr\left[P_\alpha\left(s_0, s_1\right)P_\beta\left(r_{0,\beta}\left(\mathbf{u}\right), r_{1,\beta}\left(\mathbf{u}\right)\right)\right] + Tr\left[P_\alpha\left(s_0, s_1\right)P_\alpha\left(r_{0,\alpha}\left(\mathbf{u}\right), r_{1,\alpha}\left(\mathbf{u}\right)\right)\right]\right] \\
&= \frac{1}{p^2}\left[-1 + p^2/p^2 + \delta\left(s_0, r_{0,\alpha}\left(\mathbf{u}\right)\right)\delta\left(s_1, r_{1,\alpha}\left(\mathbf{u}\right)\right)\right] \\
&= \frac{1}{p^2}\delta\left(s_0, r_{0,\alpha}\left(\mathbf{u}\right)\right)\delta\left(s_1, r_{1,\alpha}\left(\mathbf{u}\right)\right)
\end{aligned}
$$

Thus, $W_\rho\left(\mathbf{u}\right)$ equals $1/p^2$ on those p^2 four-vectors which match the given phases and equals zero elsewhere. For $\alpha \neq p^2$, $r_{k,\alpha}\left(\mathbf{u}\right) = -Da_1 + \mathbf{u}\circ\mathbf{g}_k\left(\alpha\right)$, and it can be shown easily that the set of four-vectors satisfying those conditions is

$$\{\mathbf{u} = b_0\mathbf{g}_0\left(\alpha\right) + b_1\mathbf{g}_1\left(\alpha\right) + (0, s_0 + Da_1, 0, s_1 + Da_1) : b_0, b_1 \in GF(p)\}.$$

That is, $W_\rho\left(\mathbf{u}\right)$ is constant on a shift of the two-dimensional subspace indexed by α. An analogous result holds if $\alpha = p^2$, and, as expected, this parallels the situation when $n = 1$.

D. Separability of the Wigner function for p=2

When $p = 2$ Eq. (54) can be used to define the Wigner function with the definition of the characteristic function given in Eq. (62) below. Properties other than separability follow as

before, but the analysis leading to separability for p odd does not work in this case. The discussion above made use of the existence of a quadratic non-residue D; however, for $p = 2$ no such quantity exists. In addition we must include the factors of $\alpha_2 = \alpha_2(1,1) = -i$ defined at the end of III.

Explicit forms of generating vectors are

$$G_{a_0,a_1} = \{(1, a_1, 0, a_0 + a_1), (0, a_0 + a_1, 1, a_0)\}$$

for $\alpha = a_0 + a_1\lambda \in GF(2^2)$, and

$$G_4 = \{(1, 0, 0, 0), (0, 0, 1, 0)\}.$$

For the case $\alpha \neq 2^2$, the analog of Eq. (52) is

$$\chi_\rho(\mathbf{w}) = Tr[\rho(\alpha_2^{a_1}\eta^{r_0}S_{\mathbf{g}_0})^{b_0}(\alpha_2^{a_0}\eta^{r_1}S_{\mathbf{g}_1})^{b_1}] \tag{62}$$

where r_0 and r_1 depend on a_0 and a_1. It is convenient to write the index equation Eq. (57) in the form

$$\mathbf{w} = (b_0, q_0) \oplus (b_1, q_1) = b_0\mathbf{g}_0(\alpha) + b_1\mathbf{g}_1(\alpha),$$

then it is not difficult to show that for $(b_0, b_1) \neq (0, 0)$

$$a_0 = b_0q_0 + (b_0 + b_1)q_1$$
$$a_1 = (b_0 + b_1)q_0 + b_1q_1.$$

This allows us to replace the sums in the Wigner function over a_0 and a_1 by sums over q_0 and q_1. Now we can write

$$\chi_\rho(\mathbf{w}) = \eta^{(b_0r_0+b_1r_1)}\alpha_2^{(b_0q_0+b_1q_1)}\eta^{b_0b_1(q_0+q_1)}Tr[\rho S_{b_0,q_0} \otimes S_{b_1,q_1}]. \tag{63}$$

As stated above, we require that the phase factors are linear in the b's. In order to enforce this it is easy to show that if $r_0 = 0$ and $r_1 = a_0 = b_0q_0 + b_1(a_0 + a_1)$ the exponent of η is simply b_1q_1. This calculation makes use of the binary arithmetic, in particular $b^2 = b$.

Finally, we find that for $\rho = \tau \otimes \mu$ the phase factor $\eta^{b_1q_1}$ requires that we use different one particle Wigner functions for the two particles. Equivalently,

$$W_\rho(u^{(0)} \oplus u^{(1)}) = W_\tau(u^{(0)})W_{\mu^t}(u^{(1)})$$

where μ^t is the transpose of the qubit density matrix μ. If we had taken $r_0 = a_1$ and $r_1 = 0$ the transpose would have appeared on τ, rather than on μ.

E. Separability and Partial Transposition

A necessary condition for separability of a density matrix of a bipartite system $\rho \in H_p \otimes H_p$ is the Peres condition [18]. That is, the density matrix must transform into a density matrix under partial transpose

$$PT: \quad \langle j_0, j_1 | \rho | k_0, k_1 \rangle \rightarrow \langle j_0, k_1 | \rho | k_0, j_1 \rangle \tag{64}$$

The transpose of a spin matrix is given by $(S_{j,k})^t = \eta^{-jk} S_{j,p-k}$; consequently, under the PT transformation

$$\chi(b_0 u_q^{(0)} \oplus b_1 u_r^{(1)}) \rightarrow \eta^{-rb_1} tr \left[\rho S_{u_q^{(0)}}^{b_0} \otimes S_{u_{p-r}^{(1)}}^{b_1} \right].$$

Therefore,

$$PT: \quad W(\mathbf{u}) = W\left(u^{(0)}, u^{(1)}\right) \rightarrow W\left(u^{(0)}, p - (u^{(1)} + 1)\right)$$

Unfortunately, this is not very useful since proving that W corresponds to a density matrix is not simple, see X G.

VIII. WIGNER FUNCTION: $d = p^n$.

The generalization to p^n degrees of freedom, where p is prime, is based on the Galois field (see $GF(p^n)$ [20] and Appendix X B). Starting from Eqs. (39) and (40), the set of vectors in C_α defined on the phase space $V_2(p^n)$ generates a MUB. As before $\mathbf{u}$ denotes a vector in $V_{2n}(p) = \bigoplus_{j=0}^{n-1} V_2^{(j)}(p)$ that we also write as $\mathbf{u} = \bigoplus_{j=0}^{n-1} u^{(j)}$ where $u^{(j)} \in V_2^{(j)}$. These indices define the tensor products of spin matrices by $S(\mathbf{u}) = \otimes_{j=0}^{n-1} S_{u^{(j)}}$. We also use the vector symplectic product introduced in Eq. (42). When $p = 2$ we need the usual factor of $-i$ if $u^{(j)} = (1, 1)$.

The basic structure of the classes of indices defined by the mapping M is discussed in section VI and Appendix X B. Specifically, class C_α of $V_2(p^n)$ maps onto an n-dimensional subspace of $V_{2n}(p)$. Each subspace is spanned by a set of n vectors G_α as defined in Eq. (43) that depend explicitly on the parameters $\alpha = (a_0, a_1, \ldots, a_{n-1})$ in $GF(p)$ which define α in $GF(p^n)$ as a vector over $GF(p)$. Since $\mathbf{u} \circ \mathbf{v} = 0$ for any two vectors in C_α, it follows $\mathbf{g}_r(\alpha) \circ \mathbf{g}_s(\alpha) = 0$ for two generating vectors.

As in the case of $n = 1$ and $n = 2$, each non-zero vector in one of the C_α is mapped into a $\mathbf{w} \neq \mathbf{0} \in V_{2n}(p)$ that can be written uniquely as

$$\mathbf{w} = \sum_{j=0}^{n-1} b_j \mathbf{g}_j(\alpha).$$

Assume p is odd. Following the paradigm established earlier, for a given density ρ define

$$\chi_\rho(\mathbf{w}) = Tr\left[\rho\left(\eta^{r_0} S_{\mathbf{g}_0(\alpha)}\right)^{b_0} \cdots \left(\eta^{r_{n-1}} S_{\mathbf{g}_{n-1}(\alpha)}\right)^{b_{n-1}}\right]. \tag{65}$$

A discrete Wigner function for a density ρ on H^{p^n} is defined

$$W_\rho(\mathbf{u}) = \frac{1}{p^{2n}} \sum_{\mathbf{w}} \eta^{\mathbf{u} \circ \mathbf{w}} \chi_\rho(\mathbf{w})$$

where $\mathbf{u} \circ \mathbf{w}$ is defined in Eq. (42).

It is not difficult to show that $W_\rho(\mathbf{u})$ is real and $\sum_{\mathbf{u}} W_\rho(\mathbf{u}) = 1$. The proof is simply a matter of keeping track of the various representations:

$$
\begin{aligned}
W_\rho(\mathbf{u}) &= \frac{1}{p^{2n}} \left[1 + \sum_\alpha \sum_{(b_0,\ldots,b_{n-1}) \neq (0,\ldots,0)} \eta^{\sum_j \mathbf{u} \circ (b_j \mathbf{g}_j(\alpha))} Tr\left[\rho(\eta^{r_0} S_{\mathbf{g}_0(\alpha)})^{b_0} \cdots (\eta^{r_{n-1}} S_{\mathbf{g}_{n-1}(\alpha)})^{b_{n-1}}\right]\right] \\
&= \frac{1}{p^n}\left[-1 + \frac{1}{p^n} \sum_\alpha Tr\left[\rho \prod_j \sum_{b_j=0}^{p-1} \left(\eta^{(\mathbf{u} \circ \mathbf{g}_j(\alpha) + r_j)} S_{\mathbf{g}_j(\alpha)}\right)^{b_j}\right]\right] \\
&= \frac{1}{p^n}\left[Tr\left(\rho\left[-I + \sum_\alpha P_\alpha(\mathbf{u} \circ \mathbf{g}_j(\alpha) + r_j)\right]\right)\right].
\end{aligned}
$$

This immediately confirms that W_ρ is real and shows that $W_\rho(\mathbf{u})$ is the coefficient of the Hermitian matrix $A_{\mathbf{u}} = (-I + \sum_\alpha P_\alpha(\mathbf{u} \circ \mathbf{g}_j(\alpha) + r_j))/p^n$.

For the normalization, summing over $\mathbf{u}$ is equivalent to summing over all of the vectors in each α summand:

$$\sum_{\mathbf{u}} W_\rho(\mathbf{u}) = \frac{1}{p^n}\left[-p^n + \sum_\alpha Tr(\rho I)\right] = 1$$

as required. Again note that we inserted a factor of η^{r_k} into the $g_k(\alpha)$ term to define a set of Wigner functions. This latitude of definition is exploited in the Appendix to give complete separabilty when p is an odd prime. Furthermore, with this *special* choice of phase factors, the analog of Eq. (48) holds and the generalization of the argument for $n = 2$ gives

$$A(\mathbf{u}) = \bigotimes_{j=0}^{n-1} A(u^{(j)}),$$

31

where $\mathbf{u} = \bigotimes_{j=0}^{n-1} u^{(j)}$.

For $p = 2$ the same calculations apply provided factors of $-i$ are included where required. However the methodology establishing separability fails for $n > 2$, and as far as we can determine the Wigner function as defined above does not respect separability.

IX.   DYNAMICS

For completeness, we conclude with a discussion of Hamiltonian dynamics in the present context. Starting from the Heisenberg - von Neumann equation for a $d-$dimensional system.

$$\frac{d\rho}{dt} = i\,[\rho, H] = i\,(H\rho - \rho H)\,. \tag{66}$$

($\hbar = 1$) we obtain a closed form for the dynamics of either the Wigner function or the characteristic function when $d = p$, a prime.

Let p denote an odd prime. The spin coefficients of a density ρ are defined by

$$s_u = tr\left(S_u^\dagger \rho\right) \tag{67}$$

so that

$$\rho = \frac{1}{p}\left[\sum_u s_u S_u\right]. \tag{68}$$

In defining the Wigner function, however, we emphasized the role of the characteristic functions $\chi_\rho\,(mu_a)$ rather than the spin coefficients, and we also noted that one could add phase factors. For this discussion we use

$$\chi_\rho\,(mu_a) = \begin{cases} tr\left(\rho\left(\eta^{2^{-1}a}S_{u_a}\right)^m\right) & a \neq p \\ tr\left(\rho\left(S_{u_p}\right)^m\right) & a = p \end{cases}$$

since the extra phase factors simplify the analysis. The same convention will be used for the Hamiltonian H. Of course, the spin function and characteristic function are simply related. Using Eq. (22), we obtain for $y = (y_0, y_1) = mu_a$

$$s_y = \eta^{2^{-1}y_0 y_1}\chi_\rho\,(-y)\,, \tag{69}$$

and the phase factors allow us to avoid making $a = p$ an exceptional case in (69). Thus (68) becomes

$$\rho = \frac{1}{p}\sum_u \eta^{2^{-1}u_1 u_0}\chi_\rho\,(-u)\,S_u. \tag{70}$$

32

Since the spin matrices are orthogonal, it is easy to show that

$$\frac{d\chi_\rho(-w)}{dt} = i \sum_u L(w,u)\chi_\rho(-u) \tag{71}$$

where

$$L(w,u) = \frac{1}{p}\chi_H(u-w)\left(\eta^{2^{-1}w\circ u} - \eta^{2^{-1}u\circ w}\right). \tag{72}$$

Equation (69) enables one to convert (72) to describe the dynamics in terms of the spin coefficients rather than the characteristic functions. It is easy to check that L is a Hermitian operator indexed by $V_2(p)$, so that (71) can be solved in closed form.

The evolution of the system can also be expressed in terms of the evolution of the Wigner functions. Using Eq. (25) together with the results above, we avoid explicit use of the $A(u)$ operators. Since the Wigner function is real, using Eq. (24)) we can write

$$W_\rho(v) = \frac{1}{p^2}\sum_w \eta^{v\circ w}\chi_\rho(w) = \frac{1}{p^2}\sum_w \eta^{w\circ v}\chi_\rho(-w). \tag{73}$$

Then taking the time derivative, using (72) and then inverting (73) gives

$$\frac{dW_\rho(v)}{dt} = i\sum_v \tilde{L}(v,y)W_\rho(y), \tag{74}$$

where

$$\tilde{L}(v,y) = \frac{1}{p}\left[\eta^{2v\circ y}\chi_H(2(y-v)) - \eta^{2y\circ v}\chi_H(2(v-y))\right] \tag{75}$$

is Hermitian on $V_2(p)$.

This representation works best when the density ρ evolves in the convex hull of the MUB projections. As an example when $p=3$, let the Hamiltonian be

$$H = \omega\left(S_{0,1} + S_{0,1}^\dagger\right)$$

and take $\rho(0)$ to be $P_{(1,1)}(0) = \frac{1}{3}[S_{0,0} + S_{1,1} + \eta S_{2,2}]$. Computing L and finding its spectral decomposition leads to the expression of $\rho(t)$ in terms of MUB projections as

$$\rho(t) = \frac{1}{3}[(1+2\cos(\omega t))P_{(1,1)}(0) + (1+2\cos(\omega t + 2\pi/3))P_{(1,0)}(1)$$
$$+ (1+2\cos(\omega t + 4\pi/3))P_{(1,2)}(2)].$$

In the special case of $p=2$, the necessity of selectively introducing a factor of $-i$ modifies the form of L. Any density ρ can be written as

$$\rho = \frac{1}{2}[\sigma_0 + m_x\sigma_x + m_z\sigma_z + m_y\sigma_y]$$
$$= \frac{1}{2}[S_{0,0} + s_{0,1}S_{0,1} + s_{1,0}S_{1,0} + s_{1,1}S_{1,1}].$$

where $s_{0,1} = m_x$, $s_{1,0} = m_z$ and $s_{1,1} = -i m_y$, and the $m's$ are real with square sum less than or equal to 1. Defining the characteristic function as before,

$$\chi_\rho (j, k) = Tr \left[\rho \left(\alpha_{j,k} S_{j,k} \right) \right],$$

we find $\chi_\rho (u)$ equals the corresponding m and

$$s_{j,k} = (-i)^{jk} \chi_\rho (j, k).$$

Working through the differential equation leads to a similar form:

$$\frac{d\chi_\rho (v)}{dt} = i \sum_u L(v, y) \chi_\rho (y) \tag{76}$$

with L a Hermitian matrix given by

$$L(v, y) = \frac{1}{2} \chi_H (v + y) \left[(i)^{y \diamond v} - (i)^{v \diamond y} \right]. \tag{77}$$

Thus the structure of L is similar to the $p > 2$ case but with powers of i rather than powers of $\eta = -1$. That difference makes the corresponding equation for the Wigner function more complicated, and we do not present it here. Our conclusion is that the discrete Wigner function is not particularly useful for studying the dynamics of a two-level system.

A similar approach works for n systems, and we record the results for $n = 2$. For $\mathbf{u} = u^{(0)} \oplus u^{(1)} = b_0 \mathbf{g}_0 (\alpha) + b_1 \mathbf{g}_1 (\alpha)$ set

$$\chi_\rho (\mathbf{u}) = \begin{cases} Tr \left[\rho \left(\eta^{2^{-1} y_{00}} S_{\mathbf{g}_0} \right)^{b_0} \rho \left(\eta^{2^{-1} y_{11}} S_{\mathbf{g}_1} \right)^{b_1} \right] & \alpha \neq p^2 \\ tr \left(\rho \left(S_{\mathbf{g}_0} \right)^{b_0} \left(S_{\mathbf{g}_1} \right)^{b_1} \right) & \alpha = p^2 \end{cases}$$

where for $\alpha \neq p^2$ we use $\mathbf{g}_0 (\alpha) = (1, y_{00}, 0, y_{01})$ and $\mathbf{g}_1 (\alpha) = (0, y_{10}, 1, y_{11})$. Recall that $y_{01} = y_{10}$. One can then prove for all cases of α that

$$\chi_\rho (-\mathbf{u}) = \chi_\rho^* (\mathbf{u})$$

and setting $u^{(k)} = \left(u_0^{(k)}, u_1^{(k)} \right)$

$$s_{\mathbf{u}} = \eta^{2^{-1} \left(u_0^{(0)} u_1^{(0)} + u_0^{(1)} u_1^{(1)} \right)} \chi_\rho (-\mathbf{u}), \tag{78}$$

again for all α.

Recall the vector symplectic product

$$\mathbf{u} \circ \mathbf{w} = \left(u^{(0)}, u^{(1)}\right) \circ \left(w^{(0)}, w^{(1)}\right) = \sum_{k=0}^{1} u^{(k)} \circ w^{(k)},$$

and for convenience set $\langle \mathbf{u}, \mathbf{u} \rangle = u_0^{(0)} u_1^{(0)} + u_0^{(1)} u_1^{(1)}$. Then

$$\rho = \frac{1}{p^2} \sum_{\mathbf{u}} \eta^{2^{-1}\langle \mathbf{u},\mathbf{u}\rangle} \chi_\rho(-\mathbf{u}) \, S_{\mathbf{u}}. \tag{79}$$

Using the analogous representation for the Hamiltonian, we have the analogue of (71):

$$\frac{d\chi_\rho(-\mathbf{w})}{dt} = i \sum_{\mathbf{u}} L(\mathbf{w}, \mathbf{u}) \chi_\rho(-\mathbf{u}), \tag{80}$$

where

$$L(\mathbf{w}, \mathbf{u}) = \frac{1}{p^2} \chi_H(-\mathbf{w} + \mathbf{u}) \left(\eta^{2^{-1}\mathbf{w} \circ \mathbf{u}} - \eta^{2^{-1}\mathbf{u} \circ \mathbf{w}} \right) \tag{81}$$

is Hermitian on $V_4(p)$.

The derivation of the dynamics in terms of the Wigner functions follows almost word for word the pattern in the $n = 1$ case, since the computation of the Wigner function in terms of the characteristic function is symbolically identical. This time

$$\tilde{L}(\mathbf{v}, \mathbf{z}) = \frac{1}{p^2} \left[\eta^{2\mathbf{z} \circ \mathbf{v}} \chi_H(2\mathbf{v} - 2\mathbf{z}) - \eta^{2\mathbf{v} \circ \mathbf{z}} \chi_H(2\mathbf{z} - 2\mathbf{v}) \right] \tag{82}$$

is Hermitian on $V_4(p)$ and

$$\frac{dW_{\mathbf{v}}}{dt} = i \sum_{\mathbf{z}} \tilde{L}(\mathbf{v}, \mathbf{z}) W_{\mathbf{z}}. \tag{83}$$

When $p = 2 = n$, we obtain a structurally similar result, although as before powers of i appear instead of powers of η. Letting $u^{(k)} = \left(u_0^{(k)}, u_1^{(k)}\right)$ and $\mathbf{u} = u^{(0)} \oplus u^{(1)}$,

$$\chi_\rho(\mathbf{u}) = (-i)^{\langle \mathbf{u},\mathbf{u}\rangle} s_{\mathbf{u}}$$

and

$$\frac{d\chi_\rho(\mathbf{w})}{dt} = i \sum_{\mathbf{u}} \left(\frac{1}{4} \chi_H(\mathbf{w} + \mathbf{u}) \left[i^{u \circ w} - i^{w \circ u} \right] \right) \chi_\rho(\mathbf{u}).$$

The operator in the sum is Hermitian, and again the transformation to the Wigner function context does not seem to be particularly useful.

Acknowledgments

X. APPENDICES

A. Finite fields

Reference [14]

A finite field K is a finite set of elements that contains an additive unit 0 and a multiplicative unit 1, that K is an Abelian group with respect to addition, $K^* = K - \{0\}$ forms an Abelian group under multiplication, and the usual associative and distributive laws hold. The simplest example of a finite field is the set of integers modulo a prime number p that is denoted by $Z_p = \{0, 1, \cdots, p - 1\}$. If p is not prime there are elements that do not have inverses, for example the set $Z_4^* = \{1, 2, 3\}$ does not form a multiplicative group because $2^2 = 0 \mod 4$.

It can be shown that if K is a finite field, then $|K|$, the number of elements in K, is p^n, the power of a prime. Fields with the same number of elements are isomorphic and are generically denoted as the Galois field $GF(p^n)$. A field containing p^n elements, $n > 1$, can be constructed using an irreducible polynomial f of degree n that has coefficients in $GF(p) = Z_p$. Let

$$f(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$$

be such a polynomial. Let $\lambda \notin GF(p)$ denote a symbolic root of $f(x) = 0$ so that

$$\lambda^n = -\left(c_{n-1}\lambda^{n-1} + \ldots + c_1\lambda + c_0\right). \tag{84}$$

It can be shown that each element in $GF(p^n)$ can be represented as

$$\alpha(\lambda) = \sum_{k=0}^{n-1} a_k \lambda^k. \tag{85}$$

Addition and multiplication proceed in the usual manner with the replacement of powers of λ greater than $n - 1$ reduced by using Eq. (84). While the explicit representation depends on the choice of f, the theory guarantees different representations are isomorphic.

As an example, we saw in Section VI that if $n = p = 2$, then $f(x) = x^2 + x + 1$ and $GF(4) = \{0, 1, \lambda, \lambda + 1\}$. For p an odd prime and $n = 2$ we noted that elements of $GF(p^2)$ could be written as $j + k\lambda$, where j and k are in $GF(p)$ and $f(x) = x^2 - D$ with D a quadratic non-residue mod$p$.

In addition, there is a *trace* operation defined on $GF(p^n)$ that is linear over $GF(p)$ and that maps $GF(p^n)$ to $GF(p)$. Specifically, if $\lambda_0, \ldots, \lambda_{n-1}$ denote the n distinct roots of f, then

$$tr(\alpha(\lambda)) \equiv \sum_{r=0}^{n-1} \alpha(\lambda_r).$$

The elements α in $GF(p^n)$ can thus be viewed as a vector space over the field $GF(p)$ with basis $\{\lambda^k : 0 \le k < n\}$. A *dual basis* $\{g_k(\lambda) : 0 \le k < n\}$ can be defined such that elements of $GF(p^n)$ also can be written as a linear combinations of the g_k's with coefficients in $GF(p)$. The definition of a dual basis uses the trace operation with the requirement that

$$tr\left[\lambda^j g_k(\lambda)\right] = \delta(j, k).$$

This structure was described in the Appendix of [20] and the complete theory is presented in [14].

B. Mutually unbiased bases for d=p^n.

For the finite field $GF(p^n)$, as is explained in section VI, we start with a vector space $V_2(p^n)$. We need to map the vectors in $V_2(p^n)$ onto the space $V_{2n}(p)$ in order to write out the spin matrices corresponding to the set of MUB. A typical vector βu_α can be written as

$$\beta u_\alpha = \sum_{j=0}^{n-1} \left(x^{(j)}(\alpha, \beta)e_j + y^{(j)}(\alpha, \beta)f_j\right). \tag{86}$$

The $x^{(j)}(\alpha, \beta)$ and $y^{(j)}(\alpha, \beta)$ are in $GF(p)$ and $\{e_j, f_k : 0 \le j, k < n\}$ is a set of $2n$ linearly independent vectors over $GF(p^n)$. It is convenient to take them to be of the form $e_j = \lambda^j(1, 0)$ and $f_k = g_k(\lambda)(0, 1)$ so that

$$tr(f_k \circ e_j) = tr\left(\lambda^j g_k(\lambda)\right) = \delta(j, k).$$

The key point to defining a MUB is that for two non-zero vectors in $V_2(p^n)$, say $\gamma_1 u_\alpha$ and $\gamma_2 u_\beta$, $\gamma_1 u_\alpha \circ \gamma_2 u_\beta = 0$ iff $\alpha = \beta$. Consequently, if in Eq. (86) we set $x_r^{(j)} = x^{(j)}(\alpha, \beta_r)$

and $y_r^{(j)} = y^{(j)}(\alpha, \beta_r)$ for $r = 1$ and 2, we have

$$
\begin{aligned}
0 &= tr\left(\beta_1 u_\alpha \circ \beta_2 u_\alpha\right) \\
&= tr\left(\sum_{j=0}^{n-1}\sum_{k=0}^{n-1}\left(x_1^{(j)}e_j + y_1^{(j)}f_j\right) \circ \left(x_2^{(k)}e_k + y_2^{(k)}f_k\right)\right) \\
&= \sum_{j=0}^{n-1}\left(y_1^{(j)}x_2^{(j)} - x_1^{(j)}y_2^{(j)}\right) \\
&= \sum_{j=0}^{n-1}\left(\left(x_1^{(j)},y_1^{(j)}\right) \circ \left(x_2^{(j)},y_2^{(j)}\right)\right).
\end{aligned}
\tag{87}
$$

Identifying the jth vector as the indices of the jth spin matrix in an n-fold tensor product, we have a necessary and

sufficient condition for commutativity:

$$
\otimes_{j=0}^{n-1}S_{x_1^{(j)},y_1^{(j)}} \otimes_{k=0}^{n-1}S_{x_2^{(k)},y_2^{(k)}} = \otimes_{k=0}^{n-1}S_{x_2^{(k)},y_2^{(k)}} \otimes_{j=0}^{n-1}S_{x_1^{(j)},y_1^{(j)}}.
$$

Thus the set of p^n vectors $\{\gamma u_\alpha, \ \gamma \in GF(p^n)\}$ corresponds to a commuting class $\mathfrak{M}_\alpha$ of p^n tensor products of spin matrices. The linear mapping $M : V_2(p^n) \rightarrow V_{2n}(p)$ defined by

$$
M\left(\sum_j(x^{(j)}e_j + y^{(j)}f_j)\right) = \left(x^{(0)}, y^{(0)}, \ldots, x^{(n-1)}, y^{(n-1)}\right)
\tag{88}
$$

is one-to-one and onto. Using Eq. (87) this partitions the generalized spin matrices into $d + 1$ commuting classes having only the identity in common and satisfying the condition for the existence of a set of $d + 1$ mutually unbiased bases. In writing the M mapping we are using a different definition of the basis $\{e_j, f_j\}$ that the one used in [20]. The definition in this paper lends itself more readily to a discusion of separability.

C. Separability and the M mapping

We provide some details about the mapping $M : V_2(p^n) \rightarrow V_{2n}(p)$. Let λ denote a root of an nth order irreducible polynomial over $GF(p)$. On $V_2(p^n)$ recall the set of vectors

$$
\{e_j = \lambda^j(1,0), \ f_j = g_j(\lambda)(0,1), \ j = 0, 1, \cdots, n-1\}
$$

where $tr(f_j \circ e_k) = \delta(j,k)$. Let $\alpha = \sum_{j=0}^{n-1} a_j \lambda^j \in GF(p^n)$ and using Eq. (86) define

$$u_\alpha = (1, \alpha) = e_0 + \sum_{j=0}^{n-1} y_j^{(0)}(\alpha) f_j$$

$$y_j^{(0)}(\alpha) = \sum_{k=0}^{n-1} \left(tr\lambda^{j+k}\right) a_{k.} \tag{89}$$

Then for $l = 1, \cdots, p-1$

$$\lambda^l u_\alpha = e_l + \sum_{j=0}^{n-1} y_j^{(l)}(\alpha) f_j$$

where

$$y_j^{(l)}(\alpha) = \sum_{k=0}^{n-1} tr\left(\lambda^{j+l+k}\right) a_k. \tag{90}$$

Let us work out the details for the case p an odd prime and $n = 2$. We choose as our irreducible polynomial $x^2 - D = 0 \bmod p$, where D is a quadratic non-residue. The symbolic roots of this equation are λ and $(p-1)\lambda$. For example if $p = 3$ we may take $D = 2$. Then $tr[f(\lambda)] = f(\lambda) + f(2\lambda)$. It is not difficult to show $g_0(\lambda) = 2^{-1}$ and $g_1(\lambda) = (2D)^{-1}\lambda$. Then

$$y_0^{(0)} = 2a_0, \ y_1^{(0)} = y_0^{(1)} = 2Da_1, \ y_1^{(1)} = 2Da_0.$$

We now can define the index generators of the MUB by

$$G_\alpha = \left\{ \mathbf{g}_r(\alpha) = M(\lambda^r u_\alpha) = \bigoplus_{j=0}^{n-1} u_r^{(j)}(\alpha), \quad u_r^{(j)}(\alpha) = (\delta(j,r), y_r^{(j)}), \ r = 0, 1, \cdots, n-1 \right\}$$

$$G_{p^n} = \left\{ \mathbf{g}_r(p^n) = \bigoplus_{j=0}^{n-1} u_r^{(j)}(p^n), \quad u_r^{(j)}(p^n) = (0, \delta(j,r)), \ r = 0, 1, \cdots, n-1 \right\}. \tag{91}$$

We should note that $\mathbf{g}_r(p^n)$ is not $M(\lambda^r(0,1))$ but rather $M(g_r(\lambda)(0,1))$. For the example of odd p and $n = 2$ we find for $\alpha = a_0 + a_1\lambda$, $a_0, a_1 \in GF(p)$,

$$G_\alpha = \left\{ \mathbf{g}_0(\alpha) = (1, 2a_0) \oplus (0, 2Da_1), \ \mathbf{g}_1(\alpha) = (0, 2Da_1) \oplus (1, 2Da_0) \right\}$$

$$G_{p^2} = \left\{ \mathbf{g}_0(p^2) = (0,1) \oplus (0,0), \mathbf{g}_1(p^2) = (0,0) \oplus (0,1) \right\} \tag{92}$$

Each generator set is characterized by two independent four-vectors that determine a plane containing p^2 points. These planes intersect at only one point, the origin, and so the $p^2 + 1$ sets determine $p^2 - 1$ distinct points and, including the origin, every point of $V_4(p)$.

We note from Eqs. (89) and (90) that $y_k^{(j)} = y_j^{(k)}$ which ensures the symplectic product is preserved by the mapping. Therefore, we have for the general case

$$\lambda^r u_\alpha \in V_2(p^n) \to \bigoplus_{j=0}^{n-1} u_r^{(j)}(\alpha) \in V_{2n}(p) \to S_{\mathbf{g}_r(\alpha)}^b \equiv \bigotimes_{j=0}^{n-1} S_{u_r^{(j)}}^b \tag{93}$$

where $u_r^{(j)}$ depends on α and the b_j. With this notation, the mapping from the index space to the spin matrices is complete,

$$G_\alpha \to \mathfrak{M}_\alpha = \left\{ \prod_{r=0}^{n-1} S_{\mathbf{g}_r(\alpha)}^{b_r} = \bigotimes_{j=0}^{n-1} \prod_{r=0}^{n-1} S_{u_r^{(j)}}^{b_r}, \quad b_r \in GF(p) \right\}.$$

For the case of an odd prime p and $n = 2$ this result is Eq. (47).

The spin matrices can be further expanded with the help of Eqs. (10) and (12), the symmetry of the $y_r^{(j)}(\alpha)$, and a lot of algebra. First

$$\bigotimes_{j=0}^{n-1} \prod_{r=0}^{n-1} S_{u_r^{(j)}(\alpha)}^{b_r} = \bigotimes_{j=0}^{n-1} S_{b_j, q_j(\alpha)} \eta^{\Phi_j(\alpha, b)} \tag{94}$$

$$q_j(\alpha, b) = \sum_{r=0}^{n-1} b_r y_j^{(r)}(\alpha),$$

$$\Phi_j(\alpha, b) = \left(2^{-1} b_j (b_j - 1) y_j^{(j)}(\alpha) + b_j \sum_{r=0}^{j-1} b_r y_j^{(r)}(\alpha) \right). \tag{95}$$

If $b_j \neq 0$, define $q_j(\alpha, b) = b_j q_j'(\alpha, b)$ and we have

$$S_{b_j, q_j(\alpha, b)} = S_{1, q_j'(\alpha, b)}^{b_j} \eta^{-2^{-1} b_j (b_j - 1) q_j'(\alpha, b)}.$$

If $b_j = 0$, we have

$$S_{0, q_j(\alpha, b)} = S_{0,1}^{q_j(\alpha, b)}$$

After some manipulation, we can then rewrite Eq. (94) as

$$\bigotimes_{j=0}^{n-1} \prod_{r=0}^{n-1} S_{u_r^{(j)}(\alpha)}^{b_r} = \eta^{\Theta(\alpha, b)} \bigotimes_{b_j \neq 0} S_{1, q_j'(\alpha, b)}^{b_j} \bigotimes_{b_j = 0} S_{0,1}^{q_j(\alpha, b)} \tag{96}$$

where the proper order of the tensor products is understood and where

$$\Theta(\alpha, b) = 2^{-1} \sum_r b_r \sum_{j \neq r} y_j^{(r)}(\alpha) - 2^{-1} \sum_{b_j = 0} q_j(\alpha, b). \tag{97}$$

We now can incorporate the factor Θ into the definition of χ as is done in Eqs. (51) and (65). Again leaving the ordering of the tensor products understood, Eq. (96) can be rewritten as

$$\prod_r \left(\eta^{-2^{-1}\sum_{j\neq r} y_j^{(r)}(\alpha)} S_{\mathbf{g}_r(\alpha)} \right)^{b_r} = \bigotimes_{b_j \neq 0} S_{1,q'_r(\alpha,b)}^{b_j} \bigotimes_{b_j=0} \left(\eta^{-1/2} S_{0,1} \right)^{q_j}. \tag{98}$$

Therefore, we have shown that by introducing an appropriate phase factor that depends on r and α with each $S_{\mathbf{g}_r(\alpha)}$ and by using $\eta^{-2^{-1}} S_{0,1}$ in the definition of the one particle Wigner function, we can define a Wigner function for all $n > 1$ that respects complete separabilty for odd p. Note that the spin matrices appearing in the direct product are all in the standard form S_{u_c} where $c \in I_p$.

For the example of odd prime p and $n = 2$ we have for b_0 and b_1 not equal to zero

$$q_0(\alpha, b) = b_0 2a_0 + b_1 2Da_1, \quad q_1(\alpha, b) = b_0 2Da_1 + b_1 2Da_0$$
$$\Theta(\alpha, b) = (b_0 + b_1)2Da_1. \tag{99}$$

As stated in Section VII D the analysis for $p = 2$ requires special handling. For the case of a bipartite system, it was shown in VII D that we could still prove a form of separability; however, for $n > 2$ we have been unable to make the method used here work.

D. Symplectic structure of the MUB

We have seen that Eq. (91) determines the index sets for the MUB. If $u, v \in V_2(p^n)$, consider the transformations $A : V_2(p^n) \rightarrow V_2(p^n)$ that leave the symplectic product $u \circ v$ invariant. This is the set of 2×2 matrices with entries in $K = GF(p^n)$ with unit determinant which forms the symplectic group $Sp(2, K)$ [5, 10, 24].

We now want to study the mapping M defined in section VI. For simplicity we take $n = 2$ so that the sets of generators of the MUB on $V_4(p)$ are $\{\mathbf{g}_0(\alpha), \mathbf{g}_1(\alpha)\}$. Introduce the 2×2 matrix $\sigma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and the 4×4 matrix $J = \begin{pmatrix} \sigma & 0 \\ 0 & \sigma \end{pmatrix}$, then we can write the symplectic product in terms of an ordinary inner product, $\mathbf{g}_0(\alpha) \circ \mathbf{g}_1(\alpha) = (\mathbf{g}_0(\alpha), J\mathbf{g}_1(\alpha))$. Let $A \rightarrow A_4$ where A_4 is a linear transformation on $V_4(p)$, such that $A_4\mathbf{g}_0(\alpha) \circ A_4\mathbf{g}_1(\alpha) = \mathbf{g}_0(\alpha) \circ \mathbf{g}_1(\alpha)$. Then a matrix representation of A_4 must satisfy $A_4{}^t J A_4 = J$, where $A_4{}^t$ is the transpose of A_4. The set of linear transformations that satisfy this condition forms the symplectic group $Sp(4, Z_p)$. This is analogous to the canonical transformations for the continuous case. Under

such a transformation, the classes C_α determining the ONB of a given MUB are mapped into one another. In summary, the symplectic group $Sp(2, p^n)$ can be mapped onto a symplectic group $Sp(2n, Z_p)$ and the operators A_{2n} act on the bases in a MUB in such away as to leave the MUB invariant. For further discussion of the symplectic group in this context see [24].

E.   Phase Space and Finite Geometry.

The purpose of this section is to review the role played by the geometry of the phase space. In Section IV we defined $V_2\,(p)$ to be the phase space for the discrete Wigner function when $n = 1$, and lines in the vector space play an important role in relating the Wigner function to probability measurements. By analogy, for $d = p^n$ a natural candidate for phase space for a d -level system is a two dimensional vector space with entries from an appropriate set of scalars which has d elements in it; that is, we consider $V_2\,(p^n) = \left\{ (\alpha, \beta) : \alpha, \beta \in GF(p^{n)} \right\}$. However, in analogy with the continuous case for n each described on a Hilbert space H_p we use $V_{2n}(p)$ as the phase space. The M mapping takes lines in $V_2(p^n)$ to hyperplanes in $V_{2n}(p)$.

If K denotes a finite field, the definition of a line in $V_2\,(K)$ is the obvious one. A line L in $V_2\,(K)$ is a set of points in $V_2(K)$

$$\{(x, y) : -\lambda y + \mu x + \gamma = 0 \ x, y \in K\}.$$

We always omit the case in which $\lambda = \mu = 0$. It is important to note the line consists of these points and only these points. For example in $V_2(3)$, the sets $L_1 = \{(0,0), (1,1), (2,2)\}$, $L_2 = \{(0,0), (1,2), (2,1)\}$, and $L_3 = \{(0,1), (1,2), (2,0)\}$ are lines. Two lines intersect only if they have a point in common, otherwise they are parallel. The lines L_1 and L_2 in the above example intersect at the origin, while L_1 and L_3 are parallel.

$V_2\,(K)$ is also an example of an *affine plane*, a concept defined axiomatically in terms of a finite number of points, a finite number of lines, and the relationship that a point lies on a line. It can be shown that if a finite affine plane AP exists, then there is an m such that AP has exactly m^2 points, $m^2 + m$ lines, each line contains m points and each point is on $m + 1$ lines. Two lines are said to be *parallel* if they have no point in common, and there are $m + 1$ sets of m parallel lines. (See [14] for a summary of these results and references.) Since no affine plane is known for an m which is not a power of a prime, we are again restricted

to dimension p^n.

The image under M of lines in $V_2 (p^n)$, play a central role in the definition of a Wigner function, and we summarize a few of their properties. Using the generalization of Eq. (31) with $GF(p^n)$ replacing Z_p we have:

$$L(\alpha, \gamma) = \{xu_\alpha + \gamma u_d : x \in GF(p^n)\}$$
$$L(p^n, \gamma) = \{yu_d + \gamma u_0 : y \in GF(p^n)\}$$

with $\alpha, \gamma \in GF(p^n)$. Recall that $u_\alpha = (1, \alpha)$, and $u_{p^n} = (0, 1)$. The vectors u_α and u_d multiplying the variables x or y were introduced earlier in Eq. (39) as a convenience. They now are playing the role of "slopes" in an indexing of lines in $V_2 (p^n)$, a much more general setting. For each slope, as γ varies over $GF(p^n)$ we get a set of parallel lines that contains each point in $V_2(p^n)$ once.

1. Each line contains p^n elements, and there are $p^{2n} + p^n$ distinct lines.

2. The lines through the origin, $L(\alpha, 0)$ where $\alpha \in I_{p^n} = GF(p^n) \cup \{p^n\}$, only intersect at the origin. Furthermore,

$$\bigcup_{\alpha \in I_{p^n}} (L(\alpha, 0) - \{(0, 0)\}) = V_2 (p^n) - \{(0, 0)\} .$$

3. Each set of parallel lines partitions $V_2(p^n)$:

$$V_2 (p^n) = \bigcup_{\gamma \in GF(p^n)} L(\alpha, \gamma)$$

for each $\alpha \in I_{p^n}$.

The relevance to this paper of the affine plane is that it can be shown that for certain values of d, such as $d = 6$, there is no corresponding affine plane, and for other values of d, such as $d = 12$, the existence of a corresponding affine plane is an open question. (See standard texts in combinatorics for more details or [8] for references.) We have already noted that if K denotes a finite field, then $V_2 (K)$ is an example of an affine plane, so we are working in the most general context with the necessary structure.

The last tool we need is the symplectic product of vectors in $V_2 (K)$ over the finite field K. Specifically, recall that

$$(\mu_1, \nu_1) \circ (\mu_2, \nu_2) = \nu_1 \mu_2 - \mu_1 \nu_2, \tag{100}$$

where the algebra is in the field K. As an example, $u_\alpha \circ u_\beta = 0$ if and only if $\alpha = \beta$. For each $\alpha \neq d$ in I_d, (λ, μ) is on the line $L(\alpha, \gamma)$ where $\gamma = (\lambda, \mu) \circ u_a$.

Finally, from each u_α we generate n linearly independent vectors that are mapped into an n-dimensional hyperplane in $V_{2n}(p)$ using Eqs. (89) and (90).

F. Examples of the geometry

1. One qubit

Let $K = GF(2)$, the Galois field consisting of the integers mod 2. The six lines of $V_2(2)$ fall into three classes containing two parallel lines:

$$\{L(0,0) = \{(0,0), (1,0)\}, L(0,1) = \{(0,1), (1,1)\}\}$$
$$\{L(1,0) = \{(0,0), (1,1)\} \ , \ L(1,1) = \{(0,1), (1,0)\}\}$$
$$\{L(2,0) = \{(0,0), (0,1)\}, L(2,1) = \{(1,0), (1,1)\}\}$$

2. Two qubits

The elements of $K = GF(2^2)$ can be represented as

$$\{0, 1, \lambda, \lambda^2 = \lambda + 1\},$$

where 0 is the additive identity, 1 is the multiplicative identity, and $1 + 1 = \lambda + \lambda = 0$. The other relations follow in the obvious way, such as $\lambda(\lambda + 1) = \lambda^2 + \lambda = \lambda + 1 + \lambda = 1$. The 20 lines of $V_2(GF(4))$ fall into five classes of four parallel lines each. The class of vertical lines is generated by $L(4,0) = \{(0,0), (0,1), (0,\lambda), (0,\lambda+1)\}$, and shifts of $L(4,0)$ by $\gamma(1,0)$. The other four classes are generated by $L(\alpha,0) = \{\beta u_\alpha : \beta \in GF(4)\}$ and shifts by $\gamma(0,1)$, where $L(0,\gamma)$ corresponds to a horizontal line. Graphs of lines in $V_2(2^2)$ appear in both [13] and [29].

G. Positivity relation

We include this brief discussion in order to illustrate the difficulty in determining whether a given phase space function corresponds to a positive operator. The method given here is

closely related to the proof given in [16]. Let $\{c_{jk}\}$ be an arbitrary set of complex coefficients and define the matrix $B = \sum_{j,k} c_{jk} S_{j,k}$. Then $\rho \geq 0$ if and only if $tr(\rho BB^\dagger) \geq 0$ for all B. Writing out the sum and using the properties of the spin matrices gives

$$tr(\rho BB^\dagger) = \sum_{j,k,s,t} c_{jk} c_{st}^* tr(\rho S_{j-s,k-t}) \eta^{s(t-k)}.$$

Now we can express the trace in terms of the characteristic function

$$tr(\rho S_{x,y}) = \begin{cases} \chi(y u_p) \text{ if } \quad x = 0 \\ \chi(x u_a) \text{ where } a = x^{-1}y, \ x \neq 0 \end{cases}.$$

Therefore, we have, a not very illuminating, necessary and sufficient condition for χ to arise from a positive matrix. The necessary and sufficient condition for χ to correspond to a density matrix also requires that $\chi(0) = tr\rho = 1$.

---

[1] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, F. Vatan, Algorithmica **34**, 512 (2002), quant-ph/0103162 (Sept. 2001).

[2] P. Bianucci, C. Miquel, P. Paz, and M. Saraceno, quant-ph/0106091, (Jan. 2001).

[3] J.S. Bell, Physics **1**,195 (1964). Reprinted in J. S. Bell, *Speakable and unspeakable in quantum mechanics*, Cambridge University Press, Cambridge, 1987.

[4] A. R. Calderbank, P. J Cameron, W. M. Kantor, J. J. Seidel, Proc. London Math. Soc.**3**, 436-480 (1997).

[5] D. Fivel, Phys. Rev. Lett. **74**, 835 (1995).

[6] G. B. Folland, *Harmonic Analysis in Phase Space*, Princeton University Press, Princeton, NJ, 1989, W. P. Schleich, *Quantum Optics in Phase Space*, (Wiley-VCH, Berlin, 2001).

[7] E. F. Galvao, quant-ph/0405070, (May 2004).

[8] K. S. Gibbons, M. J. Hoffman,W. K. Wootters, quant-ph/040115 v3 (2004).

[9] M. Hillery, R. F. O'Connell, M.O. Scully, and E. P. Wigner, Phys. Rep. **106**, 121 (1984).

[10] L. K. Hua, *Introduction to Number Theory*, (Springer, New York,1982), p. 364.

[11] I. D. Ivanović, J. Phys. A **14**, 3241 (1981).

[12] M. Koniorczyk, V. Buzek, and J. Hanszky, Phys. Rev. A 64, 034301 (2001).

[13] U. Leonhardt, Phys. Rev. A **53**, 2998 (1996).

[14] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications Volume 20, Addison-Wesley, Reading MA, (1983).

[15] Longenacker and Roettler, quant-ph/0309120 (Sept. 2003).

[16] F. J. Narcowich and R. F. O'Connell, Phys. Rev. A **34**, 1 (1986).

[17] Juan Pablo Paz, Augusto Jose Roncaglia, Marcos Saraceno, quant-ph/0410117, (Oct. 2004).

[18] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[19] A. O. Pittenger and M. H. Rubin, Phys. Rev. A **62**, 032313, (2000).

[20] A. O. Pittenger and M. H. Rubin, Linear Alg. Appl. **390**, 255 (2004), quant-ph/0308142, (Aug. 2003).

[21] J. Schwinger, Proc. Nat. Acad. Sci. **46**, 570 (1960).

[22] A. Terras, *Fourier Analysis on Finite Groups and Applications*, Cambridge University Press, Cambridge, 1999.

[23] J. A. Vaccaro and D. T. Pegg, Phys. Rev. A**41**, 5156 (1990).

[24] A. Vourdas, Rep. Prog. Phys. **67**, 267 (2004).

[25] H. Weyl, *The theory of groups and quantum mechanics*, (Dover Publications, New York, 1950).

[26] E. P. Wigner, Phys. Rev. **40**, 749 (1932).

[27] W. K. Wootters, Found. Phys. **14**, 391 (1986).

[28] W. K. Wootters, Ann. Phys. **176**, 1 (1987).

[29] W. K. Wootters and B. D. Fields, Annals of Physics **191**, 363-381 (1989).